LAPPEENRANTA UNIVERSITY OF TECHNOLOGY
Department of Industrial Engineering and Management
International Operations and Marketing

MASTER'S THESIS

Wireless Technologies in E-Business:

Services, Security and Management

Master's thesis topic was approved in Industrial Engineering and Management department's meeting 12.06.2002.

Supervisor: Professor Seppo Pitkänen

Instructor: M. Sc. (Tech) Petteri Laaksonen

LAPPEENRANTA, 19.06.2002

OLLI KYTÖLÄ
MERENLAHDENTIE 48 C 12
53850 LAPPEENRANTA
FINLAND
TEL: +35850 3469 486

Olli Kytölä

ABSTRACT OF THE MASTER'S THESIS

Author:	Olli Kalervo Kytölä
Name of the thesis:	Wireless Technologies in e-Business; Services, Security and Management
Department:	Industrial Engineering and Management
Year:	2002 **Location:** Lappeenranta

Master's Thesis. Lappeenranta University of Technology

118 pages, 17 figures, 1 table, 3 appendices

Supervisor: Professor Seppo Pitkänen

Keywords: Wireless, Technology, Services, Management, Data Security

Hakusanat: Langattomat teknologiat, mobiilipalvelut, hallinta, mobiili tietoturva

Developments in new mobile devices and services have raised the interest of corporations to implement wireless applications in their own businesses. Various new technologies are broadening the possibilities for corporations to deploy new applications which also raise the requirements for the manageability. As companies implement new wireless services and applications it is important to notice the requirements for data security and its manageability.

The study defines the concept of wireless e-business and the incentives for companies to adopt wireless technologies. The study consists of the framework of wireless technologies and services today, and the security and management issues companies have to confront. This framework is then applied to a real life example of a mobile sales person to point out the related issues.

The conclusions of the study contain the current situation of the related issues with analyses for tomorrow.

DIPLOMITYÖN TIIVISTELMÄ

Tekijä:	Olli Kalervo Kytölä
Työn nimi:	Langattomat teknologiat sähköisessä liiketoiminnassa; palvelut, tietoturva ja hallinta
Osasto:	Tuotantotalous
Vuosi:	2002 **Paikka:** Lappeenranta
Diplomityö. Lappeenrannan teknillinen korkeakoulu. 118 sivua, 17 kuvaa, 1 taulukko, 3 liitettä. Tarkastaja: Professori Seppo Pitkänen	
Hakusanat: Langattomat teknologiat, mobiilipalvelut, hallinta, mobiili tietoturva **Keywords**: Wireless, Technology, Services, Management, Data Security	

Uusien mobiilien laitteiden ja palveluiden kehitys ovat herättäneet yritysten mielenkiinnon soveltaa langattomia sovelluksia omassa liiketoiminnassaan. Erilaisten tekniikoiden myötä myös mahdollisuuksien kirjo on laajentumassa, mikä johtaa erilaisten verkkojen ja laitteiden yhtenäiselle hallinnalle asetettavien vaatimusten kasvuun. Yritysten siirtyessä soveltamaan uusia langattomia palveluita ja sovelluksia on myös huomioon otettavaa sovellusten sekä palveluiden vaatima tietoturva ja sen hallittavuus.

Tutkimuksessa esitetään langattoman sähköisen liiketoiminnan määritelmä sekä kyseisien teknologioiden käyttöä edistävät tekijät. Tutkimus luo viitekehyksen yrityksen langattomien teknologioiden käytölle ja siihen olennaisesti vaikuttavista tekijöistä. Viitekehystä on käytetty todelliseen esimerkkiin, liikkuva myyntihenkilö, kyseisten teknologioiden, palveluiden, tietoturvan ja hallittavuuden näkökulmasta.

Johtopäätöksinä on arvioitu mobiilien ja langattomien teknologioiden sekä palveluiden, tietoturvan ja hallittavuuden tilaa ja analysoimalla niitä tulevaa ajatellen.

ACKNOWLEDGEMENTS

I would like to thank project manager Petteri Laaksonen for this great opportunity and for his guidance and views during the project. Also I would like to thank professor Seppo Pitkänen for his guidance and criticism.

The greatest thanks I would like to salute to the members of our project team for their valuable views and inputs to this study. Also I would like to thank you all for all those fine moments in and out of the office.

Also I would like to thank all my friends from the time of my studies in Lappeenranta University of Technology for making the time spent for studies in Lappeenranta so enjoyable.

Teemu Vuosio I would like to thank for his time for reading, correcting and commenting this thesis.

Last but not least I would like to thank my parents Anja and Valde and my sister Suvi for all their efforts for supporting me during my studies. Also I would like to thank Jouni Koivuniemi for a good fellowship and for the support and ideas for this thesis.

- Olli Kytölä -

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

This study concerns wireless technologies, services, security and management in the e-business environment, and how they can be used as tools for the electronic business.

1.1 Background of the study

Many businesses have seen dramatic changes in recent years as Internet and networked business models have changed the way companies conduct their businesses today. As the competition has got tougher many companies have implemented their own e-business strategies to gain new efficiency. Many old "Bricks and Mortar" companies are changing towards "Clicks and Mortar" in the way they conduct their businesses. Ever greater numbers of companies, even smaller ones, are seeking for ways to deploy their digital strategies.

Electronic business, as we know it now, started mainly in the United States in the 1990's in the wired networks. In the recent times the new wave of the wireless Internet boom has started from the Western Europe and Japan. By 2006 it is estimated that the number of mobile Internet users worldwide will be over 920 million and is by that time more than the number of fixed Internet users [Parker & McQueen, 2001, p. 228]

Not only are the normal consumers enjoying the new mobility as many companies have also seen the advantages of the new mobility. Many of them are eager to implement new mobile solutions to gain more efficiency for their businesses.

Implementing new wireless or mobile applications the companies also encounter new challenges like managing the mobility and also the security matters of the mobile enterprise. As there are several new kinds of wireless technologies and devices with different kinds of features they all have their own abilities and limitations for corporate usage.

1.2 Research gap and problem definition

There is a wide number of books, articles, and other sources of knowledge of different technologies, services and data security separately. Still there is only quite few of them combining all to compact piece of knowledge.

This study tries to describe all at the moment and in the near future relevant technologies and matters that corporations should consider when implementing wireless applications and services and what kind of services are already available combining them to security and managing. By giving an example case and other information there will be covered the needs and requirements for mobile services now and in the near future.

The technologies used in wireless e-business are described in Appendix I.

The key questions emerging from the research problem that need to be answered are:

- What are the current and tomorrow's main wireless technologies in Wireless e-Business? (Chapter 3)
- What are the services technologies and which wireless services are offered today for Business-to-Business and Business-to-Employee usage? (Chapter 4)
- How the security affects on Wireless e-Business? (Chapter 5)
- Are there ways to manage Wireless e-Business components? (Chapter 6)

1.3 Objectives of the study

The main objectives of this study are to chart the wireless technologies and services and explain how the security issues has to be considered in wireless e-business and how it is possible to manage the technologies, the services and the security. All of that is reflected into a case example that depicts a mobile sales person who uses wireless technologies and services to carry out his daily duties.

There will be discussed what is needed to make it possible and what are the things to be considered.

In the end there will be discussed more commonly of the wireless phenomenon and the future visions in the scope of this study.

1.3.1 Scope of the study

The scope of the study as the project it defines:
- Business sectors: business-to-business (b2b), and business-to-employee (b2e)
- Business functions: mobile professional personnel (sales, service, and maintenance personnel)

Other particular limitations concerning the scope of the study are:

- On the network technology side, the emphasis is on the radio frequency (RF) technologies
- Terminals will be covered only by their categorization and their characteristic features. More of the features are covered due to the operating systems
- Concentrates on services, management and security related matters as well as the requirements certain service applications put on these
- (Wireless) services are in this context those that enable certain corporate applications to be executed, not end level services
- Security part concentrates on the security matters that has to be considered of when implementing wireless applications
- Management part concentrates on the management of mobile devices and applications/software of a mobile enterprise

This study follows closely to the scope of the wireless e-business project with some exceptions. The project is presented in the chapter two.

1.4 Structure of the study

The structure of this study is pictured in the Figure 1.

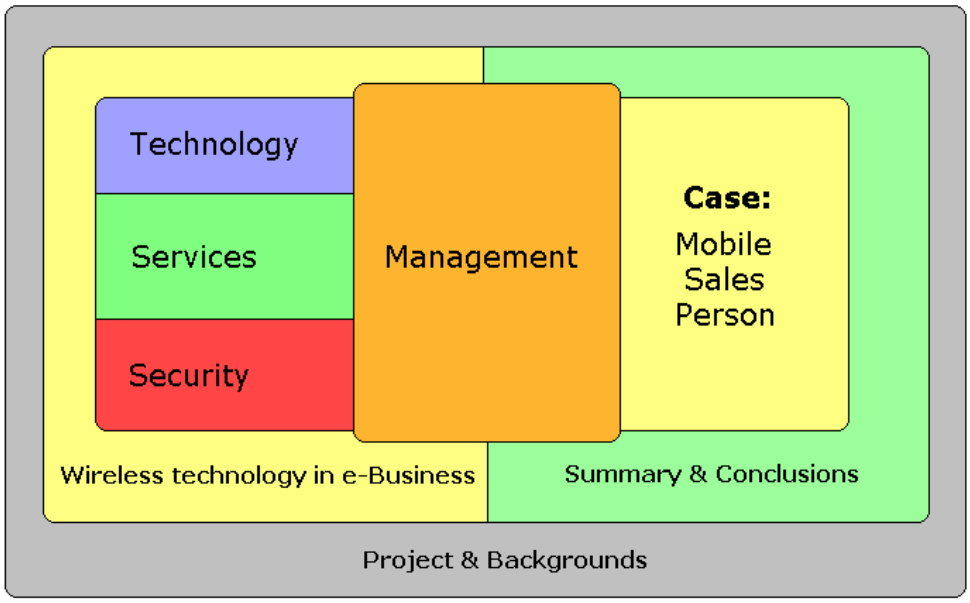


Figure 1. The structure of the study.

In the next page there is more specific structure description of this study presented in an input/output diagram. There is every chapter named in it, explained what information is needed as an input to each chapter, and described what are the supposed outcomes as results.

Table 1. The Input/Output diagram of the study.

INPUT	**CHAPTER**	OUTPUT
Background and motives Objectives Limitations	**1. Introduction**	Context & evoking interests Questions Scope Used Abbreviations
Project Drivers for mobility	**2. Introduction to wireless e-**	Give reader sights what driving companies to go

Definitions of e-business, e-commerce, etc.	**business**	mobile Give picture what is happening in near future
Networks in use today / in near future in brief Terminal technologies	**3. Wireless technologies**	Introduction of the network and terminal technologies
Service technologies Wireless services offered Service layers Requirements for mobility	**4. Wireless services**	How the technologies are used / can be used Differences in technologies and their pricing in customers point of view
Security matters Security features of networks and terminals Security policies of companies and their efficiency	**5. Wireless security**	Mobile security needs Tools for mobile security Views for security related issues
Wireless managing Problems occurred implementing wireless devices Researches carried out in companies that use mobile devices	**6. Wireless management**	Characteristics of use of the mobile devices by studies Characteristics of OS's Management of mobile personnel Views for the future needs

Earlier chapters Needs and requirements of the mobile sales person	**7. Case: Mobile sales person**	Technologies and services combined to a usable application Rising issues
Findings and results Comparisons of techs and services Application requirements	**8. Discussion, analysis and recommendations**	Needs for development Factors driving certain services Suggestions for further studies
Content of the study Conclusions	**9. Summary, and conclusions**	Summarizing the research Conclusions
	APPENDIXES	

1.5 Research methods

The methods used for collecting the information for this document have been literature readings (books, articles, Internet pages and technical white papers) and expert interviews. In the next subchapter is discussed the quality and availability of the used source's in the whole project as of in this study. The mind mapping technique was used for charting the landscape of wireless technologies (see Appendix I).

1.5.1 Literature review

The availability of relevant and topical information sources is an issue that always surfaces when doing research on leading edge topics such as e-business and mobility. This study by definition ranks among such topics and the importance of Internet and the research organizations as information sources tends to mount up at the cost of conventional literature. The rapid continual transformation in the field has the tendency of making the material outdated. These are some of the

reasons why it is important to maintain a critical approach towards the material at hand. On the other hand this may also result in the lack of available sources.

1.5.2 Interviews

During the study there were made some 20 interviews of different people of executive level in the leading companies of their own business areas in Finland, in Europe or globally. Most of the interviews were made by more than one member at the present to cover not just one study or topic made in the project "New business models arising from the convergence of e-business and mobility in the USA and Europe". Most of the interviews were recorded to a minidisk for later analysis.

1.7 Definitions and acronyms

Appendix III presents the main terms, acronyms and abbreviations used in this thesis. Also in the beginning of chapters 2 - 6 there is a more chapter specific definitions of main terms used in that chapter.

2 INTRODUCTION TO WIRELESS E-BUSINESS

The purpose of this chapter is to showcase the background of this study, the research institute where it was carried out and the project it was related to. The latter half of the chapter is focused on the appliance of the wireless technologies in the use of business and the drivers for wireless e-Business.

2.1 Background of the project

This study was made in Telecom Business Research Center in Lappeenranta University of Technology in a project called "New business models arising from the convergence of e-business and mobility in the USA and Europe".

TBRC

Telecom Business Research Center (TBRC) is the research unit of Lappeenranta University of Technology. It was established in the summer 1999 as a junction of four departments: Business Administration, Industrial Engineering and Management, Information Technology and Electrical Engineering and Electronics.

The focus area of the Telecom Business Research Center projects is the Telecom and Information Technology industry. The main aim is to connect university researchers and industry. In order to do this research groups focus on specific managerial problems and challenges.

The staff of TBRC consists of the university personnel. In other words, it is today a virtual organization of about 50 active persons. Some people from co-operating companies work in TBRC that enables the fast and effective connection with the partners.

Research teams are usually multidiscipline and consist of the researchers from different fields such as economics, information technology, telecommunications,

logistics, etc. This approach combines the technological and commercial knowledge and enables the high-level multidiscipline results.

2.2 Project and thesis

The official name of the project is “New business models arising from the convergence of e-business and mobility in the USA and Europe”. As a short name of the project used is “Wireless e-business”.

Introduction

The convergence of the IT and Telecom markets is creating completely new ways for companies to operate. The application of new technology in so-called old industries will make the Infocom sector to boom. The time window for utilizing an innovation into a new business has shrank and business-to-business e-commerce sales are developing and growing very fast.

The American way is to commercialise new business ideas fast based on existing building blocks, i.e. technology and services. Europeans move with technology standards, which easily slow down the development, but creates eventually larger standard platforms. On the other hand Europe has a major competitive advantage: the European wide GSM standard, its installation in all of the European countries and clear a evolution path. The standard platform can be utilized between business partners and within the companies own operations as well as approaching the customers.

Mobility, widely understood, opens a completely new way for companies to apply e-business in their operations.

Scope

The research program concentrates primarily on business-to-business and intra-business segments and compares the markets in the USA and in Europe. The researched companies are large industry leaders and their suppliers.

The chosen industries are:

- ICT (Information and Communication Industry)
- Paper
- Retail

Research targets of the program

1. Create a competitive Wireless E-Business research team in Finland and link it thoroughly into research in the USA.
2. Create comparative research results between the USA and Europe in application of Wireless E-Business.
3. Build co-operation between universities in Finland and in the USA.
4. Apply modelling technologies like AHP, real options etc. into fore sighting of the Wireless E-Business market development.
5. To study the new business models arising from the use of Wireless Applications.
6. Define scenarios for the E-Business development paths in Europe and in the USA and create alternative future outcomes from that. To study and model the industry restructuring in selected industry sectors due to change from Service Operator industry perspective.

Business targets of the program

1. Recognize the main benefits or opportunities for the companies in so-called old industries.
2. Analyse and forecast the speed of the change, time-to-market and growth opportunities
3. Analyse the risks or hindering factors, “stumbling stones”, delaying or stopping the possible development.

4. Define required enabling technologies and services models
5. Analyse the opportunities for new types of business models and changes to exiting ones.
6. Forecast or build scenarios of the new roles and industry structure.

Structure and phasing

The study will be divided into sub-projects, which are divided into separate research projects coordinated within this program.

The first part of the program concentrates on analyzing the present situation and strategic trends, which open new business opportunities and enable new business models. New application models are created by using the lead user method, and technical configurations and requirements are planned. New applications are analysed with a ”Return on investment” approach. The methods used are ROI, AHP and Real Options.

The second part of the program takes psychological and learning aspect in the application of the above forecasted technology and service diffusion and concentrates on taking a new aspect by finding the reasons slowing the applications of technology in organization.

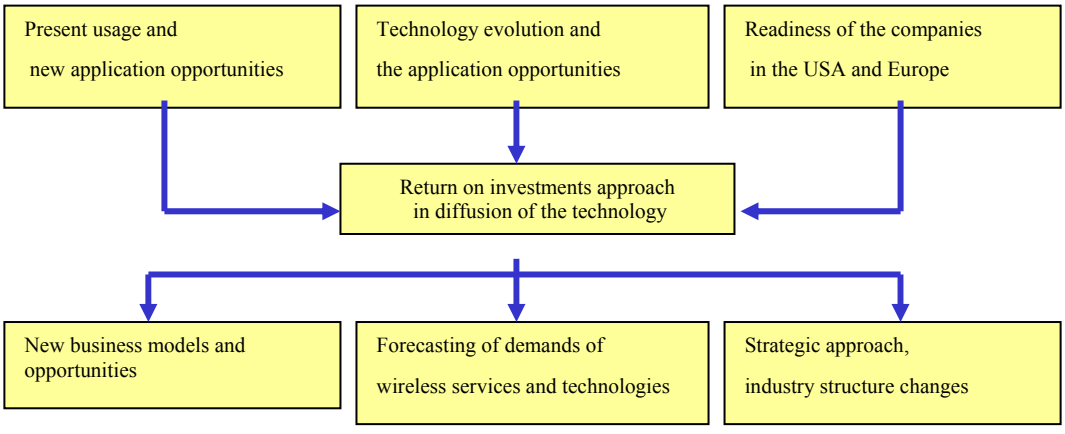


Figure 2. Structure of the project “Wireless E-Business”.

This thesis belongs to the subproject of technology evolution and the application opportunities.

2.3 Definitions

The terms, which are presented in this chapter, are shared with the project members.

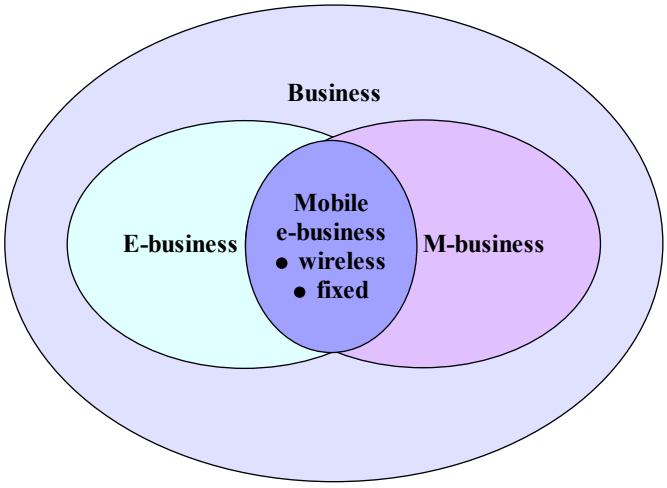


Figure 3. The convergence of E- and M-Businesses.

E-business

"Any Internet initiative - tactical or strategic - that transforms business relationships, whether those relationships be business-to-consumer, business-to-business, intra-business, or even consumer-to-consumer" [Hartman et al, 2000, xvii]

Later it is clarified that the Internet initiative can also be any electrical initiative to loosen the Internet centricity as in some E-Business applications there is no real connection to Internet e.g. Machine-to-Machine communications.

In this project e-business is defined to cover business-to-business and intra-business solutions based on electronic means of making business between business parties.

M-business

Any mobile initiative that adds demonstrable value, whether it directly results in the generation of profit or not. Traditional voice calls are not included, but services using voice recognition in order to enable commercial transactions belong into the definition.

Mobile initiative

Mobile initiative is the initiative, which uses mobile technology in the exchange of goods, services, information and knowledge

Mobile e-business

Mobile e-business is a combination of e-business and m-business. Mobile e-business solutions are accessed over Internet or some standard radio network with wire or cord alike wirelessly with mobile devices.

Application

Performs a task to provide service for an end user. Often an application is concisely viewed as a software running on a server or a handset. In the project a broadened view is applied where an application includes everything from the demand (end customer) to the source (content).

Mobile application

Mobile application is an application that can be used in anyplace in anytime where a network access is available, even a fixed one.

Mobile device

Mobile device is defined as a device that can be transported and connected to a network in different locations using wired or wireless access.

Mobility

Mobility is defined as a possibility to be connected to and get access to a network using a mobile device in different locations offering flexibility and transportability for the user.

Wireless e-business

Wireless e-business is a subset of mobile e-business. It covers only e-business solutions, which are possible to access also or only wirelessly.

Wireless

Wireless is the access to network or Internet like services in any place without wires or cords using some kind of standard radio network. Also mobile phones can be defined as wireless devices as they themselves do not need any wires or cords to get access to network.

In literature wireless is mostly associated with short distance radio technologies providing a network access locally.

Business-to-business (B2B)

Business activities between business units, companies, manufacturers, resellers (distributors, wholesalers, etc.), institutional, professional and governmental organizations. Purchases and sales to or from private consumers are excluded.

Business-to-employee (B2E)

Business activities that involve organizations and their employees. Purchases and sales are made in a role of employee or employer. The seller and the purchaser can be within the same organization or in different organizations that have business relations between them (e.g. health care services).

Machine-to-machine (M2M)

Wireless data connections between two machines, of which other can be a mobile.

Intra-business

Intra-business involves business activities inside one organization. These activities can be business-to-business, business-to-employee or machine-to-machine.

IT benefit.

"An advantage or good, something produced with the assistance of computers and communications for which a firm would be prepared to pay. In functional terms the benefits derived from IT relate to the fact that the technology allows more tasks to be completed with greater accuracy and quality in less time and for lower costs." [Remenyi et al. 1991, p. 53].

2.4 Drivers for Wireless e-Business

Although wireless technology is often linked to mobile phones, the term "wireless" actually refers to a portfolio of different technologies and architectures that enable a variety of devices to connect to each other offering the ability to exchange and synchronize data between them. Another development that is making PCs more portable and efficient is wireless local-area network (WLAN) technology. [Barbero, 2001, p. 10]

Evans suggests that businesses adopt technology and process innovations if they are deemed to add some measure of value to the enterprise. Over the years, businesses have adopted telephones, copiers, fax machines, mainframes, client-server technologies, Internet Technologies, and many other devices and technologies in order to improve communications and manage information. [Evans, 2002, p. 9]

Wireless e-business or m-commerce have not been seen as a new revolutionary revenue channel as Leung and Antapys suggest that that over the next five years, mobile commerce will produce only a fraction of the revenues wireline e-

commerce will generate over the same period. The reasons for this are mostly due to the buying behaviour and information needs to support the buying decision: the more expensive and larger the product/service to be bought is, the more it needs information to support the buying decision and vice versa. Also the small display and inconvenient input method of a mobile device puts limitations on the information supply. More likely m-commerce is for small and low priced basic or standard products which do not require much information to buy. In these circumstances it is easier to see why companies seek other use for wireless technologies like pursuing benefits of increased productivity and the flexibility of personnel's information sharing.

A driving force of the wireless revolution is the rapidly rising number of people who work at home or in mobile offices, often in collaboration with virtual items that are connected by computer networks. For sales and field service employees in particular, wireless devices allow them to stay connected and retrieve the information they need to conduct their daily business without having to return to the office to "recharge". [Barbero, 2001, p. 10]

A second motivating force behind wireless technology is its global possibilities. Due to the prohibitive costs of rolling out wireline, portable devices may be the only way to connect remote employees and companies in these areas. [Barbero, 2001, p. 10]

Companies that take the lead in the wireless revolution can position themselves as being innovative and at the forefront of the advanced technology, giving them substantial marketing leverage. Implementing wireless technology can also give organizations a competitive advantage or, at the very least, retain a level playing field with their competition. [Barbero, 2001, p. 11]

It seems fair to say that M-Business applications for the enterprise are currently in early adoption status as Evans says it. Supply of technology solutions currently outweighs demand in the enterprise, mostly because the business benefits have not

been articulated and the business value not well proven or understood. [Evans, 2002, p. 10]

2.5 Wireless technologies in e-business

In the business the use of wireless technologies has commonly been seen most beneficial for the mobile workforce but also in the offices and warehouses and even in plant environments they can bring new efficiency, flexibility and cost cutting. Sometimes it is even easier to implement wireless solutions than traditional fixed ones and the price advantage for conventional solutions may diminish or even disappear when for example the layout of the office or plant has to be revised.

The first beneficiaries of the wireless technologies have been logistics with fleet management and warehouse solutions. Another group of beneficiaries have been the field workers such as maintenance workers. Some maintenance companies use wireless technologies to track the movements of maintenance units and to dispatch them to the next destination. Paavilainen lists the advantages of mobile field services as following:

- Faster response times
- Less resource needed at the call center
- Improved dispatching process
- Streamlined workflow
- Increased efficiency of the field workers
- More statistical information available for planning
- Accurate and fast billing
- Less paperwork – less duplicated processes
- Improved communication
- On-site technical support and trouble shooting databases

[Paavilainen, 2001, p. 149]

The third group of beneficiaries have been mobile office workers such as executives and sales persons who travel around a large proportion of their work time. For example with a mobile CRM extension, a sales person is also able to perform the following tasks:

- Access inventory availability and convey the information directly to the customer
- Interact with customers, suppliers and management with a real-time connectivity
- Provide on-site price quotes
- Confirm appointments
- Access personal information management tools such as contacts and calendar
- Maintain personal sales records

[Paavilainen, 2001, p. 148]

In-Stat Group suggests that by 2004, the number of WAP users in Western Europe is estimated to grow to well over 200 million. This growth is driven by the introduction of GPRS, WAP 2.0, Bluetooth and Mobile Commerce.

Mobile services benefit from three major factors that boost information value to end users: personalisation, time-sensitivity and location awareness. Combining these elements adds even more value to the services. [Nokia, 2001a]

2.5.1 Concerns

Current challenges in the adoption of wireless technology are the security concerns and a lack of available bandwidth although the vendors and the carriers are working hard to address both issues. Other obstacles include the lack of technology standards around wireless applications, the difficulty in tailoring information and synchronizing communication between a wide range of portable devices, and a degree of uncertainty regarding the technology's financial payback.

Despite these challenges, however, companies that fail to incorporate wireless technology into the broader scheme of their overall business strategies may find themselves trailing their competitors. [Barbero, 2001, p. 11]

2.5.2 Implementation of wireless technologies

Since wireless devices are a natural extension of Internet technologies, companies can apply lessons learned from Web-based deployments to their wireless initiatives. [Barbero, 2001, p. 11]

According to Barbero companies looking to integrate wireless devices into their current infrastructure should take the three following steps:

1. Conduct an inventory of current technology to determine what exists and how much is being spent
2. Constantly raise the question of how wireless technology can be used to modify current and short term plans
3. Insure that the current or planned architecture includes wireless technology

In order for any company to successfully deploy wireless technology, top management support is critical. [Barbero, 2001, p. 12]

2.5.3 From commodity to competitive edge

The beginning of the use of wireless technologies in a company can start with a commodity product like mobile phones without substantial growth in revenue. Later it can develop into use of other products and technologies as beside the fixed corporate LAN company has a Wireless LAN that supplements the fixed LAN offering. The latest stage is gaining competitive advantage by applying wireless technologies into companies' processes where the effects of mobility and wireless technology brings more efficiency than doing things traditionally.

2.5.4 Radical new innovations

A company can adopt new innovations that are:

1. The innovation is based on mobility and wireless, or
2. The innovation is impossible to implement without wireless technology

In the first one, the new innovation is based on the benefits and possibilities of wireless technologies, but can also be implemented with traditional technologies. Still using the traditional technologies for the implementation of the innovation can lead to higher costs and vanishing benefits.

In the second one, the new innovation is based solely on wireless technology and cannot be implemented with traditional technologies. These innovations can lead to new business ideas and models.

3 WIRELESS ACCESS TECHNOLOGIES

The purpose of this chapter is to give the reader a good view of wireless technologies used today and technologies that will be adopted in the near future. Those technologies involve wireless networks and wireless terminals used for business applications and services. The emphasis is mainly on the technologies that are seen as breakthrough technologies which belong to the vital interests of different companies.

Wireless networks are divided into two classifications: to those that are managed by the operator (public networks) and to those that are managed privately by the companies themselves. Exception to this classification is Wireless LAN, which can be both, offered by some operators as well as it is possible for companies to build their own Wireless LAN network based on the same technology. The version provided by an operator is called Operator Wireless LAN (OWLAN) and they are often based on IEEE 802.11 set of standards.

Technologies will be presented shortly without going deeper into their technological backgrounds and technology itself. The purpose is to bring out the information of the possibilities of these technologies, what their advantages and disadvantages are in the context of wireless e-business applications and services.

In the Appendix II there is a table of different wireless networks used in Europe and Northern America and their typical data transfer capabilities compared.

3.1 Definitions

Hotspot	Local small area covered with a wireless network
PAN	Personal Area Network, usable for range of 10 – 100 meters
LAN	Local Area Network, usable for range of hundreds of meters

WAN	Wide Area Network, usable for range of 5 – 50 kilometres
GAN	Global Area Network, usable globally
GSM	Global System for Mobile Communications
TDMA	Time Division Multiple Access
HSCSD	High Speed Circuit Switched Data
GPRS	General Packet Radio Service
EDGE	Enhanced Data for GSM Evolution
UMTS	Universal Mobile Telecommunication System
WLAN	Wireless Local Area Network
IEEE 802.11	Institute of Electrical and Electronics Engineers standard set for Wireless LANs
ETSI	European Telecommunications Standards Institute

3.2 Public network technologies

Operator managed networks can be classified into two categories; cellular phone technologies and other network technologies.

Operator managed cellular phone technologies are in the terminology divided into generations starting in Europe from the analogue voice only networks that were called the first generation (referred as 1G). Some of the 1G networks still in use have been later tuned to be able to transfer also some data. The second generation (referred as 2G) of cellular phones are using digital technology and they have been voice centric but still offering capabilities to transfer data. The transition from second generation to third (referred as 3G) has provided or will provide some intermediate generations of cellular phone networks like 2.5G (GPRS) and 2.75G (EDGE). The main differences between 2G, 2.5G and 3G can be defined as:

2.5G is an upgrade from 2G that allows

- Higher peak data transmission rates.
- "Always on" service.

- Packet switched service (as opposed to circuit-switched as with voice).
- Additional benefit of Packet switched service: allows per-packet pricing or fixed price service.

3G differs from 2.5G in that it allows

- Even higher data transmission rates.
- Higher overall capacity (mostly because of new spectrum allocation).

[MPRG, 2001]

3G is an ITU (International Telecommunication Union) specification for the third generation (analog cellular was the first generation, digital GSM/PCS the second) of mobile communications technology. 3G promises increased bandwidth, up to 384 Kbps when a device is stationary or moving at pedestrian speed, 128 Kbps in a car, and 2 Mbps in fixed applications. 3G will work over wireless air interfaces such as GSM, TDMA, and CDMA. The new EDGE air interface has been developed specifically to meet the bandwidth needs of 3G. [Webopedia]

There are different technology evolution paths for different cellular network operators from 2G to 3G. Figure 4. shows the evolution paths.

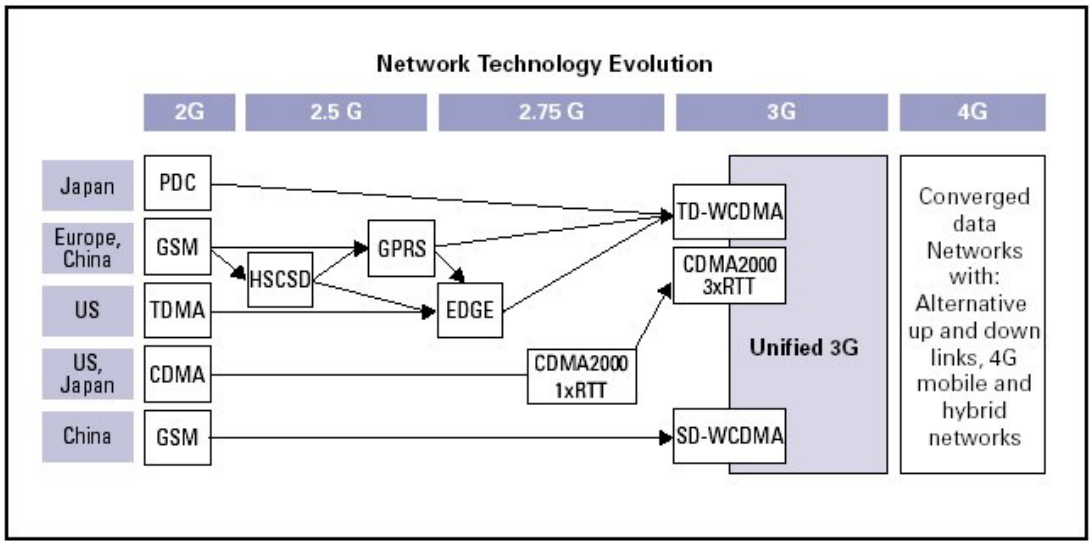


Figure 4. The network technology evolution paths from 2G to 3G [Müller-Veerse et al., 2001, p. 50]

3.2.1 GSM

GSM (Global System for Mobile Communication) is second generation (2G) mobile telephone system operating in the 900 MHz and 1800 MHz frequency band and it is the prevailing mobile standard in Europe and most of the Asia-Pacific region. GSM is also in use in the United States, but using the frequency band of 1900 MHz. [Müller-Veerse, 2001, p 19] According to GSM Association there were 564.6 million GSM subscribers by the end of July 2001 and so GSM accounts for 65.7% of the World's wireless market.

GSM standard uses TDMA (Time Division Multiple Access) for the data transfer. One TDMA frame is divided into eight time slots. Normally one GSM phone or device uses one time space at a time. In a time space given to the phone or device it transmits the data in a burst.

GSM Data is the technology to transfer binary data through GSM networks. As GSM networks are digital, all the data, including voice, is transmitted in digital format and so there is no need for modem that translates digital information to analogical information and vice versa in the other end. Normal GSM Data

transmits data using one time space at a time and so its transfer rate maximum is at the moment 9.6 kbps or 14.4 kbps depending on the device and network used.

3.2.2 HSCSD

HSCSD (High Speed Circuit Switched Data) is a circuit switched protocol based on the GSM technology. HSCSD is a technology to reach higher data transfer rates in GSM networks using multiple time slots. In HSCSD it is possible to use up to four channels at a time increasing the data transfer rate up to 57.6 kbps. [Müller-Veerse 1999, p 19]

Higher transfer rates allow more complex applications to be used as the connection speeds are near the commonly used dial-up modem connection speeds. HSCSD enables Internet and corporate Intranet surfing and receiving and sending of e-mails as well as the use of some other advanced corporate applications.

HSCSD's advantage is that the transfer rate during the usage is guaranteed as in GPRS the transfer rate is adapted to the networks other usage. Used transfer rate is selected in the beginning of the session and will be held constant through the session. HSCSD is recommendable when larger amounts of data have to be transferred in reasonable time.

Disadvantage for the HSCSD is the fact that the billing is based on the time used, not the data transferred. Even though there is no data transferred at a time when the session is on there are still costs running for the session. Also the long handshake time for HSCSD when establishing the connection is a disadvantage when comparing it against the same of the GPRS.

HSCSD has not gathered as much interest from the network operators as the GPRS has and many of the operators are directly jumping to GPRS without HSCSD. According to GSM Association there were only 32 operators in 25 countries by the end of May 2001 offering HSCSD service to 90 million possible

customers. In Finland there were only two operators offering HSCSD service at the end of September 2001, Sonera and DNA Finland.

3.2.3 GPRS

GPRS (General Packet Radio Service) is a packet switched wireless protocol as defined in the GSM standard that offers instant access to data networks. GPRS introduces three key features: always online, a convenient upgrade with instant coverage and road map to 3G. [Andersson, 2001, p. 53]

GPRS will permit burst transmission speeds of up to 107.2 Kbps when all the eight time slots are in use [Müller-Veerse, 1999, p. 20]. Generally the operators are offering at the beginning of the GPRS services only up to four time slots for use which limits the maximum transfer rate to 53.6 Kbps. Some of the operators have also to offer all eight time slot for use but only in limited areas near to the GSM base stations [DNA Finland, web pages]. Theoretically it is possible to achieve transfer rates up to 171.2 Kbps with GPRS technology [Müller-Veerse, 1999, p. 20].

In GPRS time slots are also used to achieve better data transfer capabilities, as well as in HSCSD, but the transfer rates per slot are 9.05 Kbps or 13.4 Kbps depending on network traffic and the quality of service of the network. GPRS network automatically uses the higher transfer rate but when the signal is weak, some of the bits have to be used to secure the connection and the transfer rate drops to 9.05 Kbps per slot. Also the network offers the slots depending on the traffic in the network, the heavier the traffic, the less of the slots are available for one user. [Tiainen, 2001 p. 21]

GPRS has also allowed new kind of billing and pricing compared to old circuit switched technologies. As in HSCSD the usage is billed according to the time used for the connection and maybe some fee for a session, GPRS's packet switched technology allows a more innovative billing and pricing system like

billing per quantities of transferred data, per package, per starting hour or day when data is being transferred.

GPRS's advantage over GSM Data and HSCSD is the "always on" feature that reduces the handshake time to near zero and so is recommendable for applications, such as wireless instant messaging, that need access inconstantly and the data amounts transferred are some kilobytes at a time. In GPRS the network capacity is only used when data is actually transmitted. GPRS is the first transport mode to allow full instant mobile Internet access and it is the enabler for a wide range of new application [Müller-Veerse, 2001, p. 20].

A disadvantage of GPRS against HSCSD is the cost when larger amounts of data have to be transferred constantly and the changing data transfer rates. [Kytölä & Edelmann, 2001].

In the GPRS networks voice is prioritized over the transferred data giving voice calls the capacity needed from the network. Also the first handsets are not capable of having voice and data connections simultaneously; when a call is received the data transfer will be put on hold. Later there will be handsets that are capable of transferring data during a call.

GPRS, as HSCSD, are not yet well suited for real time multimedia applications such as video conferencing and Voice over IP as they are mostly associated as wireless equivalent of analogue phone modems. Still they both enable new kind of services and applications to be used as compared to basic GSM Data. GPRS is also giving operators as well as companies possibilities to plan and test services and applications to be offered or utilized later when newer technologies, such as EDGE or UMTS, offer more bandwidth.

Lately GPRS has been accused of loose standardising leading to lack of security and poor transfer rates, as in heavier usage the transfer rates are dropped to the

levels of GSM data, about 10 kbps, without acceleration of the data by compressing it.

3.2.4 EDGE

EDGE (Enhanced Data Rate for Global/GSM Evolution) is the next step in the evolution of European GSM and also Northern American IS136. After the second generation of GSM and 2.5G GPRS, EDGE comes as the 2.75 generation (referred to as 2.75G in Europe) and, at the same time, as the third generation of TS136 (referred to as 3G in North America) [WATMAG, 2001a]. It will be available in the market for deployment by existing GSM operators during 2002 [Müller-Veerse, 2001, p.21]. The objective of the new technology is to increase the data transmission rate to open up new applications for mobile use. Whereas GPRS allows theoretically data rates of up to 171.2 kbps, EDGE is expected to offer 384 kbit/s in the same bandwidth of 200kHz. The higher data rate is the key to new applications, for example, wireless internet surfing or file transfer. EDGE also makes it possible to test some applications and services that are said to be typical for third generation networks as EDGE offers almost the same data rates as expected from UMTS at its deployment.

Some operators that own valid 3G/UMTS licences are already considering implementing EDGE as an interim data technology on the path from GPRS to UMTS, but some are even planning to jump directly from GPRS to UMTS, as the time span for EDGE before UMTS deployment seems to stay quite short and EDGE would require investments for the upgrading of existing networks. Required investments for EDGE upgrade are estimated to cost one fifth of the full roll out of the UMTS networks for GSM operators [Müller-Veerse et al., 2001, p. 51]. Other operators, which do not own any 3G/UMTS licences, can also upgrade their existing 2G networks to EDGE to compete with 3G operators as the data transfer speeds of the 3G/UMTS outside the suburban areas are expected to be somewhat the same as what EDGE will be offering. When linked to the packet-data network (PDN: IP, X25) by GPRS, this technology could become the

pacesetter in the competition with UMTS. The next generation of EDGE (GERAN) will then be able to offer services like 'voice over IP'. [WATMAG, 2001a]

After the launch of EDGE, different kinds of terminals will appear. There will be more advanced telephones and communicators, as well as more diversified versions of PDAs with integrated or add-on radio parts for connection to a network. For laptop computers there will possibly be some different kinds of solutions to connect them wirelessly to a network, the easiest being an integrated radio chip inside the device or a EDGE PC card. Other possibilities include connecting a laptop computer to a network via an EDGE capable terminal using their integrated cordless connection, for example Bluetooth or IrDA connection. The amount of different kinds of terminals that will be offered for EDGE networks will depend on how widely the operators are deploying EDGE networks. On the other hand operators' interest of deploying EDGE networks depends on how successfully GPRS and the new services are adopted by the customers and is there demand for higher transfer rates.

The success of EDGE will depend very much on the timely availability of the terminals, services and applications and how the customers adopt and use them. In suburban areas where the 3G/UMTS networks will bring more bandwidth and more complex services and applications, the opportunity window for EDGE might be short, unless major delays occur during 3G/UMTS deployment.

3.2.5 UMTS / 3G

UMTS (Universal Mobile Telecommunications Service) is a so-called "third-generation (3G)," broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 Mbps that will offer a consistent set of services to mobile computer and phone users no matter where they are located in the world. Although many people associate UMTS with a speed of 2 Mbps, this will be reached only within a networked building and indeed only with some

further development to the technology. Realistic expectations suggest a maximum capacity in metropolitan areas of 384 Kbps, at least until 2005 [Müller-Veerse 1999 p. 21]. Higher bandwidth is needed for rich multimedia content thought to be entering the market after 2005. Some sources suggest that the maximum capacity of UMTS outside the metropolitan areas will stay at the level of 384 Kbps, which can already be reached with EDGE. As EDGE is already defined in the USA as the third generation cellular system, UMTS is defined in Europe to be the first real 3G cellular system.

Based on the GSM standard, UMTS, endorsed by major standards bodies and manufacturers, is the planned standard for mobile users around the world by 2002 and 2003. Once UTMS is fully implemented, computer and phone users can be constantly connected to the Internet as they travel and, as the roaming services have the same set of capabilities no matter where they travel to. Users will have access through a combination of terrestrial wireless and satellite transmissions. Until UMTS is fully implemented, users can have multi-mode devices that switch to the currently available technology (such as GSM 900 and 1800) where UMTS is not yet available.

UMTS networks are more expensive to build than GPRS and EDGE network, as the latter ones are possible to build on existing technology and the earlier needing a whole new network infrastructure. It is said it costs 20 times more to build UMTS network as it is to update existing GSM network to GPRS [Müller-Veerse et al., 2001, p. 51]. UMTS networks operate in different frequency bands as the GSM networks. The electromagnetic radiation spectrum for UMTS has been identified as frequency bands 1885-2025 MHz for future IMT-2000 systems, and 1980-2010 MHz and 2170-2200 MHz for the satellite portion of UMTS systems. The new frequency band is also needed to make it possible to have significantly more capacity, and so better speech and quality.

As in Europe the 3G/UMTS networks will become operational during 2002 and 2003, the first 3G network is already in use in Japan since October 2001. The

NTT Docomo's 3G network works within a 30 km radius in Tokyo area offering downstream of 384 Kbps and upstream of 64 Kbps. The cost for this 3G service called FOMA (Freedom Of Multimedia Access) is about 84 USD per month and the service makes it possible to transfer live video footage if the handsets support it [eWeek, 2001]. The reasons for the earlier start of the 3G services in Japan is the congestion of 2G networks, as for example the widely successful iMode service has raised the demand for mobile network capacity. Terminal prices for the first handsets for NTT Docomo's were about 500 USD [eWeek, 2001].

3.2.6 Operator Wireless Local Area Network

Operator Wireless LANs (OWLAN) use the same technologies as in the self-managed Wireless Local Area Networks explained later. The biggest difference between the two is that when it is operated by the operator, the operator collects fees of used services, depending on the usage of the network and possibly some monthly basic fee. Some operators offer OWLAN services for companies building the network into the company's premises, taking care of the network assemblies and maintenance, giving the companies the possibility to concentrate on their own core businesses. It can also be included as a part of ASP (Application Service Provider) service.

Müller-Veerse et al. in their research [2001] believes Wireless LANs will become a public network technology that can also challenge UMTS. Many operators still see Wireless LAN as a complimentary service to existing mobile phone networks.

Operators have also deployed OWLANs into some high traffic spots like airports, sports stadiums, hotels, restaurants and conferencing rooms where the needs for data transfer is higher due to high density of people around and other wireless networks are heavily used and often congested. Good examples of Operator Wireless LANs are Sonera's wGate service and Telia's HomeRun service. It is not so farfetched to think of applying wireless networks also to service stations as

in the future also cars will have Internet access capabilities, offering it as a service among the others.

In Operator Wireless LAN service the user has a contract with the service provider and has a WLAN-capable device, often a laptop PC with WLAN card or by leasing the equipment from the service provider. Most probably there will also be some specific equipment for wireless LANs or with integrated WLAN capabilities as the amount of places, so called *hotspots*, is increasing. Identification to Operator Wireless LANs can be implemented in two ways, the first being the login password combination, and the second being a SIM (Subscriber Identity Module) card based identification as used in GSM networks. In the latter the SIM card will be installed in the WLAN PC-card, later maybe the specific devices have their own slot for the SIM card for the convenience of the user, or the card can be used in the device for both telephoning and data transfer in the same device without the need for extra SIM cards.

3.2.7 LMDS

LMDS is originally a US/FCC term meaning Local Multipoint Distribution Services. It is a frequency band in the 28 GHz range, allocated to stimulate competition in local access, and large enough, to give new operators the possibility to quickly and easily address end-users with new advanced broadband services. Today LMDS is frequently used globally as the abbreviation for what is also referred to as FWBA (Fixed Wireless Broadband Access). Frequencies for these services are being allocated globally between 24 and 31 GHz. [Ericsson, 2002]

LMDS is a so called last mile solution to provide wireless broadband network services as the typical cell size of the network is 5 km. The high frequency band and intolerance of different interferences tends to shorten the radius of a cell. In ideal conditions the cell size may even grow up to 8 km, but in Northern Europe the operator may not be able to make them much larger than 1 km to 2 km. Also

the required line of sight between the antennas of the link and the customer may set limits to the range of service [Dornan, 2001, p. 257]. The line of sight requirement also reduces the mobility within LMDS network.

LMDS is currently the fastest wireless network technology in transfer rates up to 155 Mbps, which can theoretically reach even 1-4 Gbps, as it uses a high and wide frequency band. Still often the commercially launched networks offer some tens of megabytes per second transfer rates. The used frequencies for LMDS are licensed and the transfer rates are affected by the licenses the provider has. Also the transfer capacity offered will be divided by the users, so one can not reap the whole transfer capacity for him or herself. LMDS could be a solution for densely populated areas, such as city centres or for few customers (near each other) with very high bandwidth demands.

3.2.8 Satellite systems

Satellite systems are used where no other network connections are available and it is not worth building a network. Satellite systems are useful for globetrotters and explorers, who travel through distant locations and need the communications capabilities to operate their businesses. For businesses like oil drilling, maritime logistics, research and seeking for new natural resources the usage of satellite systems is a natural choice, even though they are slower in data transfer and costly to use, but as the locations are typically where no other connections exists, they are the only options.

There are few different satellite systems operating commercially. Iridium is the system of 66 satellites orbiting 780 km above the see level covering the whole globe. Part of the system are the ground stations providing the link between satellites and ground networks. The Low Earth Orbit (LEO) satellites of Iridium offer small latency, smaller antenna sizes, and less transmission power than higher orbiting systems. Iridium offers 2.4 Kbps Dial-Up data transfer (connected to any computer) and up to 10 Kbps Direct Internet Access using Iridium Gateway

[Iridium, 2002]. The prices for usage are from about one USD/min upwards and the monthly fees about 20 USD and handsets starting from about 400 USD pagers and phones about 900 USD and up [Delta Wave Communications, 2001].

Globalstar is another LEO satellite system operating with 48 satellites orbiting at an altitude of 1.414 km and covering more than one hundred countries on six continents (see Figure 5.). Transfer rates are up to 9.6 Kbps depending on used application. [Globalstar, 2001] The costs are about the same as in Iridium as are the prices for handsets. In Finland Globalstar services are offered by Radiolinja.

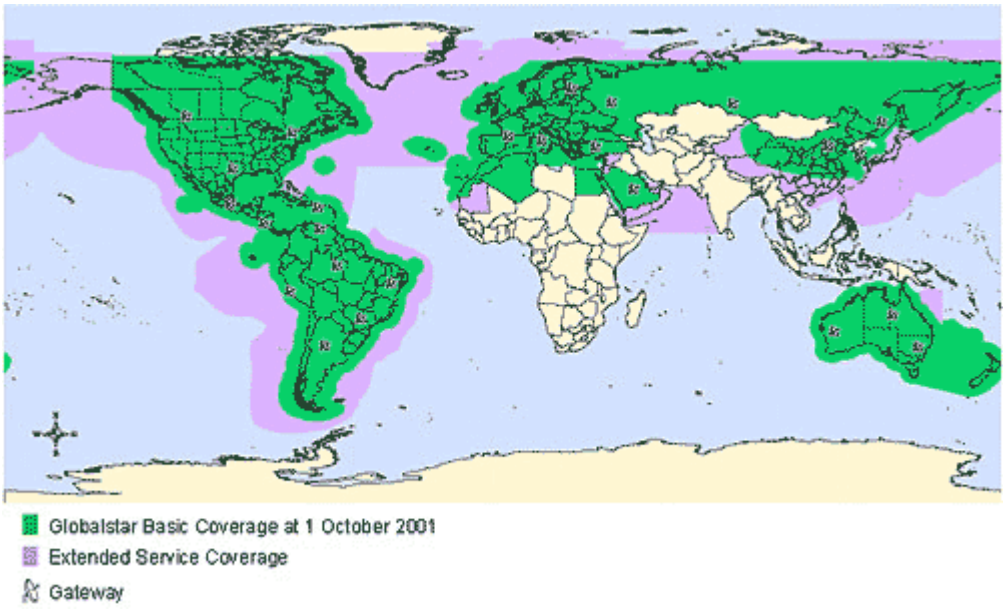


Figure 5. Coverage of Globalstar Satellite Network. [Globalstar, 2001]

Teledesic is the third mobile satellite system introduced here and the only broadband satellite system. The Teledesic Network will consist of 30 operational satellites; 12 satellites will be deployed first, providing continuous coverage in several areas of the world; 18 additional satellites will enable global coverage. The Teledesic Network is designed to support millions of simultaneous users. Multiple manufacturers will offer a family of user equipment to access the network. Using "standard" user equipment, most users will have two-way connections that provide up to 720 Mbps on the downlink and from 128 kbps up

to 100 Mbps on the uplink. The service is targeted to begin in 2005. [Teledesic, 2002]

3.3 Private wireless network technologies

Private wireless network technologies have seen the huge rise of usage and implementation during the last few years. The reasons for this can be defined as easiness of implementation (no new hard wire installations), falling technology cost, maturing technology (more and more hardware supporting these technologies and compatibility problems different devices are decreasing) and the mobility of hardware. Also one new interest for "self-managed" wireless networks has risen due to the increasing amount of mobile devices of the work force in the companies, as they need to get connected to company intranets with their devices in different locations (like different offices globally) and download the data they are needing. Those data amounts have risen in last few years dramatically, but the costs using wireless networks operated by telecoms haven't fallen as dramatically.

3.3.1 Wireless Local Area Network Technologies

Wireless Local Area Network (WLAN) technologies have been a big success in recent years as they offer easy implementation and reasonably low costs to build compared to installing fixed wired networks in small office and home environments. For older buildings the savings from building a WLAN instead of fixed network are even more tremendous. WLANs are also a valuable addition to offices that already have fixed wired networks to bring portability and flexibility to the office, which are the major drivers for building WLANs. They can also be built in environments like factories, warehouses and hospitals. Almost the only limitation to implement wireless local area networks is the imagination.

At the moment there are three main standards with their subtypes of Wireless LANs.

IEEE 802.11

In WLAN technology, 802.11 refers to a family of specifications developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). There were three specifications ready in the family by the end of 2001: 802.11, 802.11a, and 802.11b. The 802.11 and 802.11b specifications apply to wireless Ethernet LANs, and operate at frequencies in the 2.4-GHz region of the radio spectrum. Data speeds are generally 1 Mbps or 2 Mbps for 802.11, and 5.5 Mbps or 11 Mbps for 802.11b, although speeds up to about 20 Mbps are realizable with 802.11b. The 802.11b standard is backward compatible with 802.11. The 802.11a specification applies to wireless ATM systems and operates at radio frequencies between 5 GHz and 6 GHz. With the 802.11a data speeds as high as 54 Mbps are possible, but most commonly, communications take place at 6 Mbps, 12 Mbps, or 24 Mbps.

At present IEEE 802.11b seems to be the most adopted from the three for business use. Reasons for this can be listed as wide industrial adoption of the standard (multi vendor support, interoperability) and the falling technology costs as it has matured. The data transfer rate of 11 Mbps has been considered as enough for most office applications as it equals the commonly used wired Ethernet data transfer rate of 10 Mbps.

The development of the 802.11a (started) at the same time as the 802.11b but has not yet been realized in commercial products. Also due to the different frequency band 802.11a is not compatible with the older 802.11 standard and 802.11b standard.

The newest IEEE standard in the 802.11 family is the 802.11g. It can communicate also with the older standards which make it attractive for the users of the older 802.11 products. 802.11g provides data transfer rates up to 54 Mbps.

HiperLAN

HiperLAN is a set of wireless local area network communication standards primarily used in European countries. There are two specifications: HiperLAN/1 and HiperLAN/2. Both have been adopted by the European Telecommunications Standards Institute (ETSI).

The HiperLAN standards provide features and capabilities similar to those of the IEEE 802.11 wireless local area network standards. HiperLAN/1 provides communications at rates up to 20 Mbps in the 5 GHz range of the radio frequency spectrum. HiperLAN/2 operates at rates up to 54 Mbps in the same radio frequency band. HiperLAN/2 is compatible with next generation WLAN systems for sending and receiving data, images, and voice communications. HiperLAN/2 has the potential, and is intended, for world-wide implementation in conjunction with similar systems in the 5 GHz RF band.

HomeRF

HomeRF (*home radio frequency*) is a home networking standard developed by Proxim Inc. that combines the 802.11b and Digital Enhanced Cordless Telecommunication (DECT) portable phone standards into a single system. HomeRF uses a frequency-hopping technique to deliver speeds of up to 10 Mbps (HomeRF 2.0) over distances of up to 150 ft - too short a range for most business applications, but suitable for the home market that it was specifically developed for. It uses the same 2.4 GHz frequency band as IEEE 802.11b, but offers better immunity against other 2.4 GHz interference, such as microwave ovens and other WLANs than the other WLANs operating at licence free 2.4 GHz band. Also the equipment prices for HomeRF have been lower than in other WLAN technologies. HomeRF has been hurt by decreasing prices for IEEE 802.11b products as low equipment prices may be important attraction to some small businesses to adopt the technology. [HomeRF, 2001 / Kalakota & Robinson, 2001, p. 53]

3.3.2 Bluetooth

Bluetooth is a short-range radio technology that is complementary to other wireless technologies. It is expected to be integrated into hundreds of millions of devices in the future due to its small size and relatively low price.

The main requirements for Bluetooth at the start of its designing were low power needs, low costs, small footprint (size), speech and data transmission capabilities and world-wide capacity (standardization). [Andersson, 2001, p. 82] These features make Bluetooth very usable in different kinds of mobile devices to link them together almost world-wide, as only the latest of those requirements has been compromised, as some countries had already reserved the frequencies Bluetooth uses to other radio technologies. Other requirements have been met and also the price is dropping due to the increase in volumes. (At the October 2001, Bluetooth chips were priced at about 8 to 12 USD/each in large volumes and different estimates are that the price will drop below 5 USD/each by the year 2003 or 2004 depending on the source.)

Bluetooth radio technology enables any device with a chip to communicate seamlessly, even if there are non-metallic walls or other objects in the way [Andersson, 2001, p. 83]. With Bluetooth it is possible to establish small networks, so called *pico networks*. They are small networks of different devices that use Bluetooth chips to communicate with each other. These networks are categorized into Personal Area Networks (PAN) as the networks diameter is typically about ten meters, although it is possible to get as far as 100m with Bluetooth when using a stronger power.

As Bluetooth uses radio signals as its carrier, it is omnidirectional, which means that a Bluetooth signal propagates equally in all directions (see Figure 6) and you do not have to point the devices at each other as with e.g. infrared devices. While this means that Bluetooth is less sensitive to how the transmitting devices are aligned, it also opens up the risks of eavesdropping. To address this concern,

developers created an elaborative security architecture. [Andersson, 2001, p. 84] Security issues will be discussed further in Chapter 5.

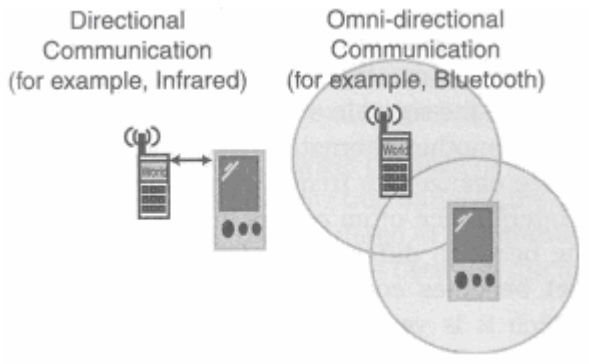


Figure 6. Omnidirectional vs. directional communication [Andersson, 2001, p. 83]

The maximum gross bit rate of Bluetooth is 1 Mbps, although protocol overhead limits the net throughput to 722 Kbps for asynchronous transfer and 433 Kbps for symmetric transfer. [Andersson, 2001, p. 84] This is enough for most applications, such as calendar synchronization, e-mail downloading, printing, small file transfer and even speech conversations, at the moment and for the next few years to come, where the Bluetooth will be applied. Bluetooth can be installed to almost any kind of computers, PDAs, mobile phones and their peripherals to bring about wireless connectivity among them.

Bluetooth operates in the 2.4 GHz *Industrial-Scientific-Medical* (ISM) frequency band (or 2402 – 2480 MHz to be exact). Each channel is 1 MHz wide, so there are 79 different channels. Bluetooth devices will coexist in the same frequency as *WLANs* and microwave ovens; consequently, the band has to be very robust. Spread-spectrum technologies help avoid interference between radio technologies. [Andersson, 2001, p. 84] Bluetooth uses frequency hopping, where the Bluetooth device changes its frequency randomly 1600 times per second. As interference often occurs in a small portion of a frequency band, hopping between the different frequencies makes channel insensitive.

In some implementations where both WLAN and Bluetooth co-exist, they divide the frequency band so they will not interfere with each other.

3.4 Wireless terminal types and technologies

Today there are hundreds of different kinds of wireless terminals on the market; mobile phones alone come in tens of different models and types. And the market seems to go to even smaller niche products, combining the different needs of specific users, e.g. Benefon's ESQ with integrated GPS (Global Positioning System) chip, making it a good choice for people needing the location data, such as truck drivers and hikers.

As the more advanced terminals resemble even more desktop and laptop PCs in their features, the operating systems that are used to operate them have become more crucial. As the competition between the PDA (Personal Digital Assistant; in our categorization all the terminal types from communicators to industrial handhelds can be included in PDA categorization) vendors have tightened in recent years, the meaning of the operating system inside the device has increased. It is also used as a marketing argument for the devices.

3.4.1 Terminal types

Different wireless terminals can be categorized from simplest to most complex as:

- One way passive terminals
- Two way passive terminals
- Pagers
- Mobile Phones
- Smart Phones
- Communicators
- Palm top computer
- Handheld computers
- Industrial handheld computers

- Tablet PC
- Laptop PC

One way passive and two way terminals can be used to send, receive, process and control data. Pagers can be used to send and receive text or character based information.

Mobile phones are mainly categorized to be able to call and receive voice calls and to have basic abilities for value added services like SMS (Short Message Service) and basic data transfer. Smart phones are like mobile phones with added features being able to simple email sending and receiving, able to read WAP (Wireless Application Protocol) pages and even modified web pages and other enhanced services.

Communicators can be defined as smart phones with handheld or PDA (Personal Digital Assistant) type of larger display and keyboard or character/handwriting recognizing display input. Also they have the most features of a PDA like word processor, spreadsheet program, email, calendar, web browser and basic multimedia presentation tools.

Palm top computers are PDAs with big touch screen display and they don't have any physical keyboard integrated to them. They can be connected to different kinds of networks through expansion cards like PCMCIA (Personal Computer Memory Card International Association) cards used in laptop PCs. Also connections to other computers can be achieved commonly through USB (Universal Serial Bus) port, serial port or via infrared connection. Generally most of their features and software depend on the operating system they are running. Most of them have the basic software for word processing, spreadsheets, presentations, multimedia, email, calendar, and web browsing. Commonly web pads are pocket sized and weigh around 200 grams, making them convenient mobile Personal Information Management (PIM) tools.

Handheld computers offer often the same features as palm top computers, but have an integrated keyboard and possibly even a larger display. Due to their size they normally have integrated PCMCIA slots, and no extension packs connected to the device itself are necessary. Handheld computers are often larger and so heavier as their counterpart palm top computers, weighing upwards from about 200 grams.

Industrial handheld computers are made for use in rougher industrial conditions. They are heavier and larger than normal handheld computers due to their protective casing. They have integrated physical or software keyboard and they often have touch screen display.

Tablet PC is a laptop PC like due to the same hardware and software base, but have no physical keyboard. Tablet PC has a big touch screen display, at least the size of DIN A4 and uses handwriting recognition tools. The same operating systems are used in tablet PCs as in laptop PCs and desktop PCs, mostly Microsoft Windows or Linux. Tablet PCs offer the same connectivity as laptop PCs; integrated PCMCIA slot, USB (Universal Serial Bus), Serial, Parallel, etc.

3.4.2 Operating Systems of PDAs

In the range of PDAs there are three main operating systems today competing for the market shares. Also some minor operating systems exist, e.g. different versions based on Linux.

Microsoft Windows CE and Pocket PC

Windows CE and Pocket PC are Microsoft's operating system for handheld and palm top computers. Pocket PC is the newer operating system as the former Windows CE got renamed as Pocket PC in the introduction of the OS version 3.0. Pocket PC is the operating system for palm top computers. For handheld computers there is a version of Windows CE called Windows for Handheld PC, which has the user interface adapted from Windows' desktop and laptop versions,

e.g. Windows 98. Pocket PC has a user interface adapted to palm top computers' smaller display.

Both of the Microsoft's operating system versions for handheld devices come with lots of features and software that are compatible with the desktop counterparts like the MS Office applications Word, Excel, Power Point, Access and Outlook and there are software tools for easy synchronisation and compatibility between the handheld device and desktop computer with Microsoft Windows.

Symbian OS

Symbian OS is Symbian's operating system designed for small, portable computer-telephones with wireless access to phone and other information services. Symbian OS is based on EPOC, an earlier operating system from Psion, the first major manufacturer of PDAs. To earlier systems, EPOC/Symbian OS adds wireless communication and architecture for adding application programs.

Symbian is a company formed by Psion, Ericsson, Nokia and Motorola. It licenses EPOC/Symbian OS to manufacturers and continues to develop it. At present there are three different versions of the current version of Symbian OS to different kinds of terminals: Quartz for palm top computers, Crystal for communicators and handheld computers and Smartphone UI for advanced mobile phones and smart phones [Symbian].

The code of Symbian OS is very compact so that it can fit on a small ROM chip. Like Pocket PC, Symbian OS comes with an "application suite," that includes a word processor, e-mail handler, spreadsheet program, a scheduling application, general purpose database, sketch program, world clock, voice recorder, spell checker, calculator, communication programs, and a Web browser. Symbian OS is also open for third party software developers. Symbian provides development kits for C++, for OPL (a BASIC-like language), and for Java.

Palm OS

Palm OS is the computer operating system that provides a software platform for the handheld PDAs made by Palm Computing (PalmPilot series) and Springboard (Visor series). Palm OS was designed from the beginning to fit into a palm-size device of a specific size and with a specific display size. 3Com, the owner of Palm Computing, says that the success of the PalmPilot series can be attributed to this special-focus approach. Microsoft's Windows CE and its successors and Symbian's EPOC/Symbian OS are designed to serve a broader range of devices.

Palm Computing chose not to include a keyboard in the PalmPilot in order to produce a truly palm-size device. PalmPilot and Visor users use instead touch screen and so called graphs, quickly learnable but restrictive set of pen strokes.

Palm OS uses multitasking as Pocket PC and Symbian OS too, but in Palm OS only one task is for applications. The user uses one application at a time, one application program must finish before the next can be selected. Palm OS comes with these applications built-in: Dates, Address Book, To Do List, Memo Pad, Calculator, and Password Protection. New applications can be written and added using several facilities that accelerate development.

Palm OS comes with communication interfaces to infrared transmission devices, TCP/IP (for Web connection through wireless or wire line devices), and, optionally, barcode recognition scanners.

Palm OS based devices have been the market leaders for many years, but have lately lost the ground to Symbian OS and Microsoft’s Pocket PC based rivals, as Palm has been criticized of slow development of features and not supporting all connectivity types enough, e.g. USB.

4 WIRELESS SERVICES

This chapter aims to give the reader a view to service technologies used in wireless services and the wireless services offered currently in business-to-business and business-to-employee categories.

4.1 Definitions

In mobile telecommunications services other than voice calls are often called as value added services (VAS). A value added service is a telecommunications service that firstly, combines the use of computers and telecommunications networks, and secondly, adds value (new functions) to the customer in comparison with the plain voice service [Leminen, 1999]

Services and applications are often used interchangeably in the literature and the distinction between them is often unclear. The following definitions of service and application are introduced for clarifying the 3G environment.

Services are the portfolio of choices offered by services providers to a user. Services are entities that services providers may choose to charge for separately. They will be key differentiators between service providers in the 3G environment. Users are likely to select their preferred 3G services providers based on the options available in that product portfolio. Different users will choose different service options. They may elect to subscribe to a personalised mobile portal offering banking facilities. They may later decide to add unified messaging. Such service options will affect the user's bill. [UMTS Forum, 2001, p. 8]

David Smith of Gartner has defined web services as following: "Services are content and software processes delivered over the Internet using loosely coupled messages (and increasingly XML interfaces) that 'service' a particular set of user needs."

Applications are service enablers – deployed by services providers, manufacturers or users. Applications are invisible to the user. They do not appear on a user's bill. A banking service, for example, would require a secure transaction application to be implemented by services provider. A unified messaging service would require voice recognition and text-to-speech applications, deployed by the network or in the terminal device. Individual applications will often be enablers for a wide range of services. [UMTS Forum, 2001, p. 8]

4.2 Key enabling service technologies

4.2.1 SMS

SMS (Short Message Service) is a character based service of sending and receiving text messages of 160 characters with a cell phone or pager. It holds significant advantages over the use of mobile email for sending important information. Originally devised as an afterthought to notify users of incoming voice mail, SMS has grown to include the sending of ring tones and graphics, as well, and taken on a life of its own. In May of 2001 alone, the GSM Association reports that 19 billion SMS were sent throughout the world.

4.2.2 EMS

EMS (Enhanced Message Service) is a developed version of the SMS. It will add new powerful functionality to the well known SMS standard, allowing mobile phone users to add life to SMS text messaging. EMS will expand the base of applications which use wireless messaging, since EMS allows the opportunity to send a combination of simple melodies, pictures, sounds, animations, modified text and standard text. Furthermore, EMS will connect the wireless world to the internet, allowing users to download pictures and ring tones to their phone. EMS

works with the existing infrastructure laid down for SMS, as well as utilizing the same familiar user interfaces and remaining compatible with existing mobile devices.

4.2.3 MMS

MMS (Multimedia Message Service) is the next step in the evolution of wireless messaging beyond text and static images and logos. MMS will depend on the formation of a new type of network infrastructure known as 3G (Third Generation), and will allow users to send messages comprised of a combination of text, sounds, images and video to MMS capable handsets [simplewire.com]. MMS provides automatic, immediate delivery of personal multimedia messages from phone to phone or from phone to e-mail.

Like SMS, MMS is an open industry standard, and MMS messages can be delivered using existing networks and protocols. MMS is bearer independent - it is not limited to GSM or WCDMA networks. [Nokia, 2001b]

4.2.4 Wireless Instant Messages (WIM)

Instant messaging (IM) is the ability to easily see whether a chosen friend or co-worker is connected to the Internet and, if they are, to exchange messages with them. Instant messaging differs from ordinary e-mail in the immediacy of the message exchange and also makes a continued exchange simpler than sending e-mail back and forth. Most exchanges are text-only. However, some services allow attachments.

Wireless Instant Messages (WIM) differs from fixed IM in the way they are transferred; on the air. Terminals are wireless smart phones, PDAs or even laptops with wireless network connection.

Instant messaging has had a huge boom in user numbers and in the traffic amounts in recent years, even more than 100% annual increase in traffic has not been rare. Still most of the instant messaging has happened in the fixed networks. New packet switched wireless networks (e.g. GPRS) are launched and new smart phones or PDAs with instant messaging software are on the markets the move to wireless instant messaging will take off and even challenge or kill the old SMS technology as the sole text messaging tool between mobile phones.

Biggest providers of instant messaging services are currently America OnLine (AOL) with its two different instant messaging software products, AOL Instant Messenger and ICQ, Microsoft by its MSN Messenger and Yahoo! with its Yahoo Messenger. All three of them already have some wireless/mobile versions of their instant messengers for mobile phones or PDAs.

4.2.5 WAP

WAP (Wireless Application Protocol) is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat (IRC). WAP protocols are largely based on Internet technologies [WAP Forum].

The WAP was conceived in 1997 by four companies: Ericsson, Motorola, Nokia, and Phone.com (former Unwired Planet) [Leung & Antypas, 2001, p. 12]. The Wireless Markup Language (WML) is used to create pages that can be delivered using WAP. WML2 is based on the eXtensible HyperText Markup Language (XHTML) developed by the W3C to replace and enhance the currently used HTML language common today. The use of Internet technologies is not new for WML, as WML1 is a fully conformant XML language in its own right [WAP Forum].

4.2.6 i-Mode

i-Mode is NTT Docomo's packet based service for mobile phones. NTT Docomo is the leading Japanese mobile operator, and sole provider of i-Mode services. Unlike the WAP, i-Mode uses a simplified version of HTML: Compact Wireless Markup Language. In the next versions of i-Mode it is planned to use XHTML as a basic language to achieve compatibility with newer versions of WAP.

As introduced in 1999, i-Mode was the world's first service for Web browsing with smart phones. i-Mode wireless data service offers colour and video over many phones. Its mobile computing service enables users to do telephone banking, make airline reservations, conduct stock transactions, send and receive e-mail, and have access to the Internet [Docomo].

4.2.7 XML

XML (Extensible Markup Language) is a formal recommendation from the World Wide Web Consortium (W3C) for describing and displaying the content. It is a structured set of rules for how one might define any kind of data to be shared on the Web. It is similar to the language of today's Web pages, the Hypertext Markup Language (HTML). Both XML and HTML contain markup symbols to describe the contents of a page or file. HTML, however, describes the content of a Web page (mainly text and graphic images) only in terms of how it is to be displayed and interacted with. XML describes the content in terms of what data is being described. This means that an XML file can be processed purely as data by a program or it can be stored with similar data on another computer or, like an HTML file, that it can be displayed.

XML is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere. Shared information on the web described with XML enables users to send intelligent

agents (programs) to those sites to gather data and then make valid comparisons. XML can be used by any individual or group of individuals or companies that want to share information in a consistent way.

XML is "extensible" because, unlike HTML, the markup symbols (tags) are unlimited and self-defining. XML is a simpler and easier-to-use subset of the Standard Generalized Markup Language (SGML), the standard for creating a document structure. It is expected that HTML and XML will be used together in many Web applications. XML markup, for example, may appear within an HTML page.

XHTML

W3C describes XHTML (Extensible Hypertext Markup Language) as being "a reformulation of HTML 4.0 as an application of the XML. It is called an "extensible" markup language because anyone can invent a particular set of markup for a particular purpose and as long as everyone uses it, it can be adapted and used for many purposes - including, as it happens, describing the appearance of a Web page.

In XHTML, all HTML 4 markup elements and attributes (the language of HTML) will continue to be supported. Unlike HTML, however, XHTML can be extended by anyone that uses it. New elements and attributes can be defined and added to those that already exist, making possible new ways to embed content and programming in a Web page. XHTML adds modularity to HTML and imposes strict conformance with the XML document structure. Modularity enables the use of extensions, and therefore, targeted content.

The members of WAP Forum have adopted XHTML Basic, a subset of XHTML, as a basis for the newest release version of WAP, WAP 2.0. XHTML Basic is the mobile adaptation of XHTML 1.0, and includes everything from the standard that is appropriate for devices with small displays. XHTML Basic is expected to become an integral part of Internet standards set.

VoiceXML

VoiceXML is an application of the XML which, when combined with voice recognition technology, enables interactive access to the Web through the telephone or a voice-driven browser. An individual session works through a combination of voice recognition and keypad entry. It allows people with an ordinary voice telephone to access the Internet to receive and send email, check sports scores, make reservations, and so on. VoiceXML can also be used in corporate systems for accessing personal e-mail and normal telephone answering machines.

VoiceXML 1.0 is an open standard. Using XML, a programmer can enable voice recognition through the addition of a few simple tags. VoiceXML can also support natural language, which means that the user is not locked into a limited script, but can speak naturally. In what is called a "modeless" or "conversational" mode, the user can even interrupt the system with an out-of-context question and thus redirect the session. The goal is to make the exchange as natural as possible, as if two humans were interacting. [Haapala, 2001]

4.2.8 Java

Java is a programming language expressly designed for use in the distributed environment of the Internet. Java can be used to create complete applications that may run on a single computer or be distributed among servers and clients in a network. It can also be used to build a small application module or applet for use as part of a Web page. Applets make it possible for a Web page user to interact with the page.

4.2.9 Positioning technologies

There are basically two ways of determining the location of a handset: a network-based solution by a mobile operator and a handset-based solution, usually done by attaching a GPS (Global Positioning System) receiver to a mobile device or

installing special piece of software into a SIM (Subscriber Identity Module) card of the mobile device. [Paavilainen, 2001, p. 178]

There are four more specific ways of providing the location information. These are: 1) Cell of Origin, 2) terminal-based, 3) network-based and 4) terminal and network –based.

Cell of Origin (COO) is the simplest way of providing the location of a subscriber as the network operator knows in which cell of its network the caller is located. The accuracy depends on the density of the cell-cites or base stations – in cities the accuracy is higher than in rural areas. Accuracy will be increased during the launch of 3G as the cell sizes will be decreased to increase the bandwidth.

Terminal-based solutions can use three different ways to determine the location of the handset: 1) GPS, 2) software residing on a SIM card with phones supporting SIM Toolkit or 3) software residing in the mobile terminal. GPS is accurate (<100 meters horizontally and 156 meters vertically) but slow and high in battery consumption due to the use of satellites to determine the location (at least three satellites is needed to determine the location). In addition, GPS can only be used outdoors as buildings and tunnels may block the connections to satellites. Also high prices, bigger sizes and other requirements make GPS unattractive to mobile device manufacturers'. Therefore GPS is not opted in use of personnel the cities but is primarily used in fixed objects as cars, boats and shipments, in order to provide high accuracy. The other way of determining the location on the terminal base is using specific software that calculates the time differences of the sent and received data. The software can reside in either on the device itself or on its SIM card. In the software based solution the accuracy depends on the density of the base stations.

Network-based solutions use various techniques to determine the location of the mobile device. Currently the accuracy of network-based solutions varies between 100 and 200 meters, but the accuracy is expected to increase with future network

technologies. Network-based solutions are also more expensive than Cell of Origin and terminal-based methods as operators need to upgrade their existing networks.

Terminal and network-based solutions use both, the terminal positioning and network positioning to increase the accuracy also outside the urban areas where the cell sizes can be up to 30 km of diameter. Network assisted GPS, for example, is used for high accuracy in both rural and urban areas. Due to use of GPS, the same problems with devices occur as with devices solely using GPS making it useful in fixed objects like cars and shipments. It can be used to locate taxi drivers, valuable assets, trains and workforce utilizing cars such as service and maintenance personnel.

4.3 Wireless Service Platforms and Architectures

4.3.1 Definitions

Middleware

Middleware is a general term for any programming that serves to "glue together" or mediate between two separate and usually already existing programs. A common application of middleware is to allow programs written for access to a particular database to access other databases.

Messaging is a common service provided by middleware programs so that different applications can communicate. The systematic tying together of disparate applications is known as enterprise application integration (EAI).

Platform

A platform is any base of technologies on which other technologies or processes are built.

Architecture

In information technology, especially computers and more recently networks, architecture is a term applied to both the process and the outcome of thinking out and specifying the overall structure, logical components, and the logical interrelationships of a computer, its operating system, a network, or other conception. An architecture can be a *reference model*, such as the Open Systems Interconnection (OSI) reference model, intended as a model for specific product architectures or it can be a specific product architecture, such as that for an Intel Pentium microprocessor or for IBM's OS/390 operating system.

4.3.1 Microsoft's .NET

.NET is Microsoft's platform for XML Web services. XML Web services allow applications to communicate and share data over the Internet, regardless of operating system or programming language. .NET Platform includes a comprehensive family of products, built on XML and Internet industry standards that provide for each aspect of developing, managing, using, and experiencing XML Web services. [Microsoft, 2001]

.NET is not a standard, it is more of a business strategy that is aimed at a convergence of personal computing with the Web. The goal is to provide individual and business users with a seamlessly interoperable and Web-enabled interface for applications and computing devices and to make computing activities increasingly Web browser-oriented. The .NET platform will include servers; building-block services, such as Web-based data storage; and device software.

All of the details of .Net are not fully published but in general .Net platform is expected to provide:

- The ability to make the entire range of computing devices work together and to have user information automatically updated and synchronized on all of them

- Increased interactive capability for Web sites, enabled by greater use of XML rather than HTML
- A premium online subscription service, that will feature customized access and delivery of products and services to the user from a central starting point for the management of various applications, such as e-mail, for example, or software, such as Office .NET
- Centralized data storage, which will increase efficiency and ease of access to information, as well as synchronization of information among users and devices
- The ability to integrate various communications media, such as e-mail, faxes, and telephones
- For developers, the ability to create reusable modules, which should increase productivity and reduce the number of programming errors

In spring 2001 Microsoft released .NET's service concept called Hailstorm. It consists of a group of services, most important of them being Passport. Passport offers a single sign on to network and services in Passport community with one login and password combination. [Rousku, 2001] Microsoft's Passport has raised criticism against Microsoft's will to become networks' gatekeeper and also the security of Passport has raised questions, as there have been many security vulnerabilities with Hotmail service that is also a part of Passport services. In Passport it is possible to include a person's credit card information and other confidential information like logins and passwords of other services for convenient web browsing and easy transactions when buying products or services from different web services or stores.

.NET has also two rivalling architectures: Liberty Alliance Project and Open Mobile Internet Architecture Initiative. The former is formed to provide a single sign on for consumers and business users in Internet and the latter is to provide open base for business and services in mobile networks.

4.3.2 Liberty Alliance Project

The Liberty Alliance Project is a business alliance formed to deliver and support an identity solution for the Internet that enables single sign-on for consumers as well as business users in an open, federated way. [Liberty Alliance]

The primary goals of the Liberty Alliance Project are:

- To allow individual consumers and businesses maintain personal information securely.
- To provide a universal open standard for single sign-on with decentralized authentication and open authorization from multiple providers.
- To provide an open standard for network identity spanning all network devices.

[Liberty Alliance, 2001]

4.3.3 Open Mobile Internet Architecture Initiative

At the Comdex fair 2001 Nokia presented jointly with other important mobile operators and manufacturers a plan to build a common architecture and platform for services and commerce in the 3G environment. The only big names that stayed out of the co-operation were Microsoft and Qualcomm. [Tietoviikko, 15.11.2001]

The goal of the common architecture is to offer terminal independent services in all mobile networks around the globe. The architecture will be built on open standards to avoid different closed solutions of manufacturers' and operators' that are not co-operable within other networks and with all devices. [Tietoviikko, 15.11.2001]

Main goals of the initiative:

- Non-fragmented global market for the next generation of mobile services

- Participants commit to products and services based on open mobile architecture enablers
- Other companies are all welcome to join in building a common future on open standards and shared architecture

[Nokia, 2001b]

In the scope of the initiative Nokia is developing software and platforms for the services and licensing them to all other willing parties of the initiative.

For customers the initiative means that the same services are possibly at use globally, as the operators of next generation mobile networks deploy them.

4.4 Portals

Portal is a term, generally synonymous with *gateway*, for a World Wide Web site that is or proposes to be a major starting site for users when they get connected to the Web or that users tend to visit as an anchor site.

A wireless portal concentrates users around content, communications and other applications that are accessible over a wireless network using a handheld device. Portals can be divided into three categories: major general portals (Yahoo, Excite, Netscape, AOL), specialized or niche portals (Garden.com, Fool.com, Tradeineuros.com) and enterprise portals.

Typical services offered by portal sites include a directory of Web sites, a facility to search for other sites, news, weather information, e-mail, stock quotes, phone and map information, and sometimes a community forum. Some portals offer their users the ability to create a site that is personalized for their individual interests.

4.4.1 Mobile portal and multi-channel portal

Mobile portal is a term for a portal concentrated on serving mobile device users with their own services and applications. Still many traditional portals are introducing mobile or wireless versions of their offerings and are so called multi-channel portals.

An Internet portal with a mobile channel is a strong combination giving the users the possibility to choose to use the most convenient channel in different situations. These portals can also combine the location information of the mobile device to offer location based services. [Paavilainen, 2001, p. 195]

4.5 Mobile service layers and categories

4.5.1 Service Layers

Mobile services can be divided into seven layer model in figure 8. introduced by Ward [Ward, 1998, p. 56].

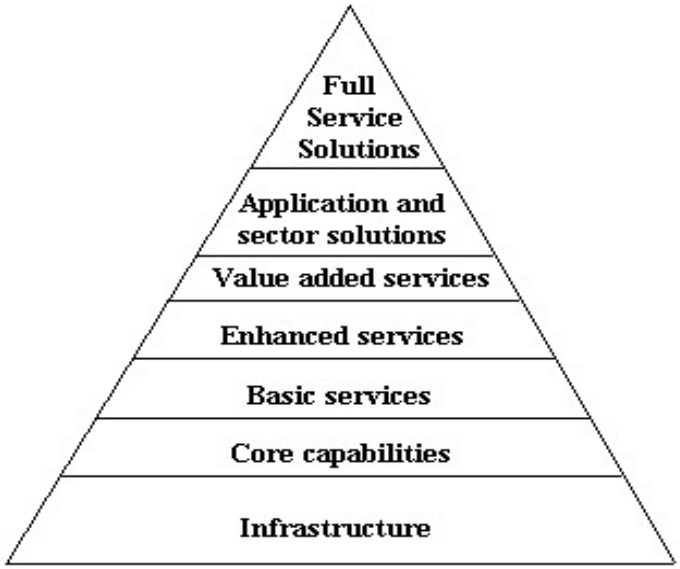


Figure 7. Seven-layer service model [Ward, 1998, p. 56]

Infrastructure provides the networks, servers and gateways, the physical part of service such as the physical WLAN implementation. *Core capabilities* present the basic data or information transmission capabilities. *Basic services* features the common services provided to a subscriber, such as voice calls, SMS messages, answering machine etc. *Enhanced services* are those that are not offered commonly but for the extra payment. Those can include EMS messaging and HSCSD or GPRS data. *Value added services* are those services that extend the functionality of basic and enhanced services. Included in this category are the subscription based services as information and infotainment services. *Application and sector solutions* are developed services for a specific industry, sector, application, or use. These services may include services or application such as SCM (Supply Chain Management) application or mobile email. *Full service solutions* represent the ability to offer complete solutions to customers for a range of telecommunications services. These solutions could comprise any number of possibilities, from all elements of the service solution being offered by the provider through their own network and internal capabilities to parts of the solution being provided by a variety of sources. The provider should handle all customer sales, service and support issues; all customer billing functions; and all negotiation and coordination functions with any other supplier or carrier involved in the customer's services.

4.5.2 Service categories

Wireless or mobile services can be divided into two sections: business and consumer market oriented services. In the scope this study we should mainly concentrate on business market oriented services (b2b-concentration) but as consumer market oriented services include some services that are covered by the business-to-employee perspective, also those will be covered.

IDC further categorizes the two sections as follows:

Business Market Orientated Services

- Intranet Access
- Internet Browsing
- Mobile Office
- Vertical Applications
- Email Access
- Machine to Machine (M2M)

Consumer Market Orientated Services

- Messaging
- Games and Entertainment
- Banking/Finance
- Location Based Services
- Internet Access (Mobile Phone)
- Information Services
- Remote Diagnostics
- Mobile Advertising
- Public Services
- Personal Health and Security

[Snellman, 2001]

4.5.1 Business market oriented services

Intranet access offers mobile access to corporate networks and their resources.

Internet browsing offers the same capabilities of searching and reading information from the Internet as normal desktop computer but on mobile devices limited screen. Maybe some of the features and capabilities cannot be used as the device in use sets the limits.

Mobile office offers the possibilities of having mobile email, calendar, contact lists and document sharing on the road. The variety of different applications available to the user may vary depending on the mobile device used.

Vertical applications are those that combine other applications through to a bigger task oriented application. Figure 8. illustrates vertical and horizontal applications.

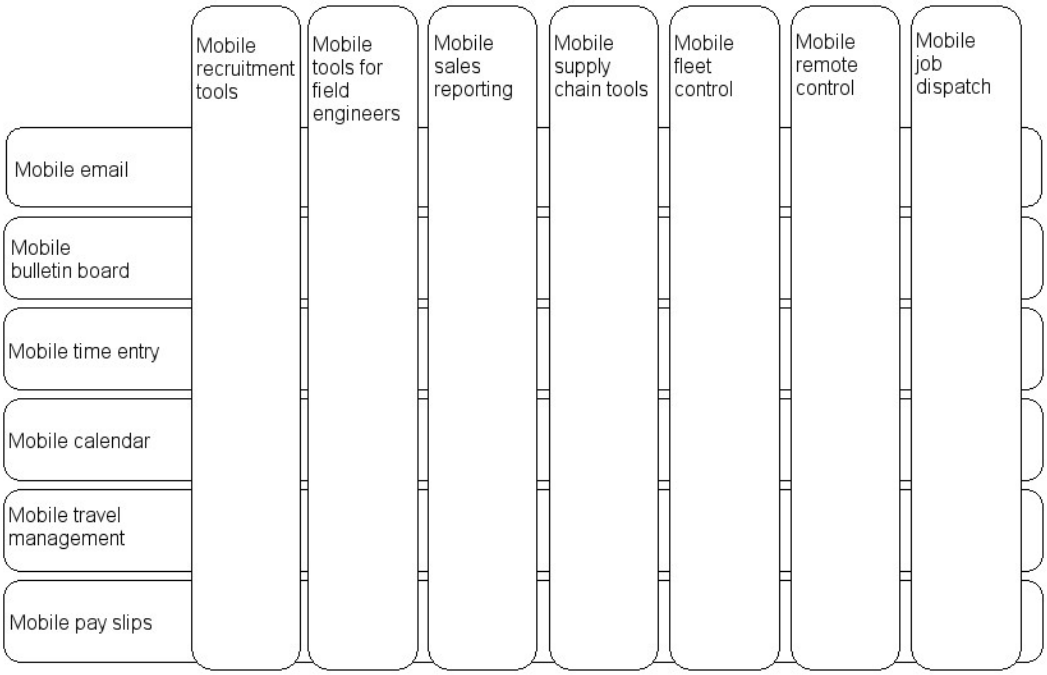


Figure 8. Vertical and horizontal applications. [Paavilainen, 2001, p. 139]

Email access can be offered as the corporate email or as another mobile only email account. Also the way how the emails can be shown depends on the device used to read the messages. For simpler devices it is normal to be able only to show plaintext messages.

Machine-to-Machine communication enables controlling and monitoring data sent across machines.

4.5.2 Business-to-Employee market oriented services

From IDC's consumer market oriented services messaging, banking/finance, location based services, internet access, information services and mobile advertising also fall into the category of business-to-employee oriented services.

Messaging through SMS has gained wide corporate acceptance to inform employees and the partners of the company of events and news. Newer comers are the instant messages that can be used for "chatting" with colleagues in different locations. First wireless instant message services are already available in USA and same kind of services are assumed to be on the European market in 2002.

Information services can offer important news (news, financial news, stock rates, exchange rates, raw material prices, etc) for the background of decision making that employees such as managers carry out in their daily routines.

Location based services can serve the employees of delivery and logistics services by guiding the route to customer or helping an employee to find to his meeting place. *Information services* companies can offer to their employees and partners can be company phone and address book, event calendar and bulletin boards. *Mobile advertising* can be used with M-CRM functions with partner groups of the company.

4.5.3 Business Applications

In the figure 9. Müller-Veerse et al. [2001] categorizes business applications to three groups. All of these can be built into services that a company offers to its own workers or to the company's partners or they can be outsourced to service providers by integrating them to their services. On the horizontal line can be seen the business-to-business interaction and on the vertical line the business-to-employee and machine-to-machine interactions of the company.

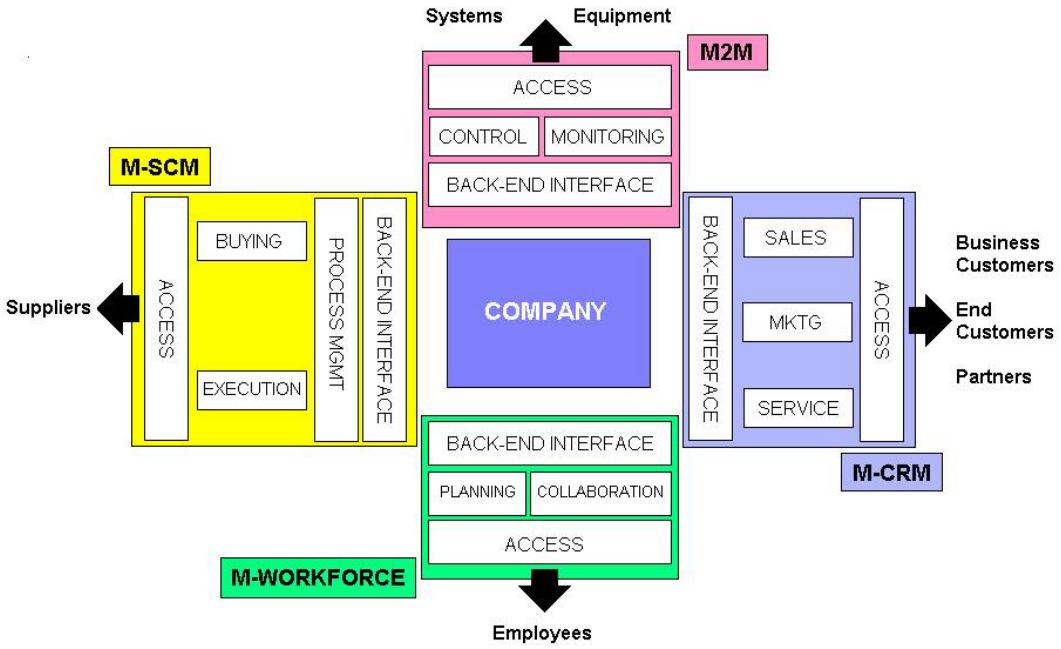


Figure 9. Business applications overview. [adapted from Müller-Veerse et al., 2001, p. 105]

4.6 Service pricing schemes in mobile environment

Till the present much of the pricing of mobile phone usage has been adopted from the old telephone operators per minute charging due to the circuit-switched technology; a circuit has to be kept open whether or not it is actually being used. It is still the predominant method of charging in both fixed and mobile phone networks. Per minute charging has not been popular among Internet surfers, as it easily leads to high usage costs while the access is narrow band. Per minute charging has also been accused of the weak success of WAP services. [Dornan, 2001, p. 165]

On the Internet, large backbone providers have also used bits based pricing for certain chunk size of data, typically megabits or gigabits, sent across their networks. This pricing is based on the old postal service, where the price of package sent is based on the weight of the package, or sometimes the volume of the package too. In the mobile phone world this is adapted to SMS messages; customers pay per message sent, not received. [Dornan, 2001, p. 165]

Pricing per bits is growing in the short term but many companies and analysts believe that neither of these pricing models is sustainable in the long term. It is believed that as the capacity will grow it will eventually become “too cheap to meter”. [Dornan, 2001, p.166] This leads to the point that in the future pricing schemes will concentrate on the access itself and the content.

Flat rate (fixed monthly charge) is already widely adopted with broadband Internet access, but still rare in the mobile networks. As the access will be flat rate the costs of transferring a single file or single call is closing to the zero. For mobile users, operators could perhaps charge small premium for mobility over the fixed network pricing.

Pay per content is already adopted by mobile operators for small contents like ringing tones, picture messages and operator logos. Because all mobile operators already have a billing system, they are easily able to charge customers micropayments – fees of only few cents for looking at specific information [Dornan, 2001, p. 166]. Then the small in size and price contents could profit the operator and the content provider noteworthily as we have seen with success of i-Mode in Japan and with the ringing tones and logos in Europe.

Operators are often willing to price their services eagerly to cover the technology costs and so the newer services provided with help of new and costly technology will be higher priced. Also the rapid evolution of the technologies has increased the speed of new technologies to come up and make older ones obsolete. In the fear of new and maybe incompatible technologies the operators need to gain back the investments made to the certain technology. This is easily seen in WLAN services based on widely deployed IEEE 802.11b as the next generation WLAN technologies are already behind the corner. Still the high pricing is scaring other than business users who don’t have to pay their usage bills themselves. Operators can use the pricing to a large extent to optimise the returns and the usage of their WLAN networks. In the usage side there are also the limitations of available radio

frequencies and so the bandwidth and the quality of service – the more users the lower the quality of service and profit margins per user.

The possible pricing schemes are shown in figure 10..

		Pricing Types				
		Metered				Unmetered
		Time based pricing	Data Volume based pricing	Value based pricing	Location based pricing	Flat-Rate pricing
Applications	Access	X	X	X	X	X
	Voice	X		X	X	X
	E-Mail		X	X		X
	Instant Messaging		X	X		X
	Content			X	X	X

Figure 10. Pricing schemes. [Müller-Veerse et al., 2001, p. 70]

The closest analogy to these new pricing schemes is to be found from the cable TV; customers pay a fixed monthly subscription fee for a limited number of channels, but are also able to access pay-per-view programming.

4.6.1 The changing operator role

Mobile phone operators have a central role in the mobile service market. They own the networks, they have the customer relationship and billing relationship to the end-user, and they have the knowledge on the customer behaviour. [Snellman, 2001, p. 30]

The first content services were rather operator centred as operators wanted to play all roles from content providing to customer relationship [Snellman, 2001, p. 30]. In recent years this model has changed a lot and is still changing as the services have split as new service and content providers have stepped into the markets.

Often new entrants have came from the media branch (print and TV) but also traditional Internet portals have started their own mobile services to attract mobile customers. Despite of these new entrants operators continue to play a significant role as utility providers. Operators strength in the game is the owned customer and billing relations, as NTT Docomo has proven with its i-Mode service, as the content of outside content providers goes through its networks to its customers and customers pay for the services through NTT Docomo. Other significant example of the changing role is the growing amount of other medias combined with mobile interactivity, such as DigiTV.

The trend of the operators concentrating from vertical service offering toward horizontal services can be seen on the figure 11.. As earlier the operators managed their services from access to end-user services as a whole, currently this is shifting to more horizontally split layers

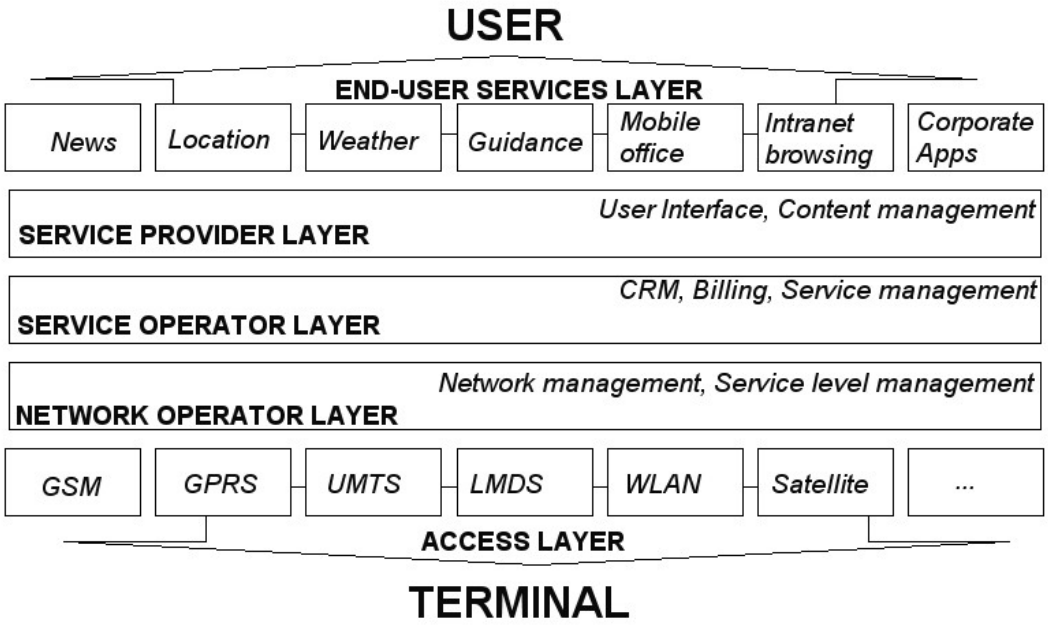


Figure 11. Horizontal service layers.

This trend is due to the fact that operators cannot concert all by themselves due to lack of resources and branch specific understanding; they focus on their own core competencies.

For customers such as corporations that use both end-user and access services this could mean easier billing through one service operator that manages centrally all the services that the user has used even though the user had used services from different service providers and networks of different network operators.

5 WIRELESS SECURITY

Wireless security is in many occasions comparable with the security of its wired equivalent. But still the mobility and increasing amount of wireless devices and networks bring new threats and make many of the old ones even bigger.

This chapter's focus is on the differences and similarities of wireless and wired security, the new threats brought by mobility, the security of networks and devices and effects of security, or lack of it. Also the ways of handling the threats will be discussed.

5.1 Definitions and acronyms used in this chapter

IPsec	Internet Protocol Security
PIN	Personal Identity Number
PKI	Public Key Infrastructure
RSA	Internet Encryption and Authentication system that uses the algorithm developed by Rivest, Shamir and Adleman, 1977
SSL	Secure Socket Layer
VPN	Virtual Private Network

5.2 Security in the new era of mobility

As the workforce is becoming increasingly mobile the security matters will rise to new dimensions. As the workplace is not necessarily inside the corporate premises in controlled and secured locations where no unauthorized persons can enter, the mobile workforce will do their work in places where also others can obtain access like public places. Still the mobile workers have needs to get access remotely to corporate intranets and databases with their mobile devices.

According to F-Secure's CEO Risto Siilasmaa the change can be seen as earlier the companies and their information systems were like fortified castles, where the

bridge over the moat could be lifted up in dangerous situations and the only threat after that came from inside. Nowadays he suggests the situation can be seen more like an airport, where anyone can have access to public spaces, but only with right access privileges one can access places like the air traffic control tower.

5.3 Security goals and needs

Basic security goals can be defined as follows:

- Availability
- Integrity
- Confidentiality

Availability consists of the information availability to the users that have the access right to that certain piece of information. For the user that has been granted the access to the information, the information should always be accessible without extra efforts made to retrieve it.

Integrity is the assurance that information can only be accessed or modified by those authorized to do so. Measures taken to ensure integrity include controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining rigorous authentication practices. Data integrity can also be threatened by environmental hazards, such as heat, dust, and electrical surges.

Confidentiality is much of privacy and trust; confidential information stays along the ones that have the rights to access that information – the data is kept private.

5.4 Security threats

The same basic security threats are confronted in fixed and wireless networks, but the wireless and mobility brings a new aspect for all of them. Due to the high and ever increasing number of wireless and mobile devices the affects can be exponential to those of the fixed ones.

The basic types and threats are:

- **attacks**
    - intellectual property theft
    - identity theft
    - brand theft
    - destruction of data and/or equipment
- **Privacy violations**
    - surveillance
    - databases collecting private information
    - traffic analysis
    - massive electronic surveillance
- **Publicity attacks**
    - disturbance or interception of communication
    - "denial-of-service" attacks

[Schneier, 2000, pp. 23-41]

5.5 Wireless security

Wireless security has lots in common with security in fixed networks as the basic rules for the both are the same – same basic tools can be used in both but many of them are more crucial to implement in the wireless world to maintain the same level of security. Wireless communications have some specific characteristics over the fixed communications that have to be considered in the sense of security. Those are:

- Transmission through air: anyone can listen (privacy)
- Radio waves do not stop to corporate walls or to other artificial borders (privacy)
- Spectrum of the radio channels is limited (availability)
- Without network coverage no services available (availability)

Keeping data private is a big issue for any wireless network. In the days of voice-only communications, the greatest worry was that an eavesdropper could listen to

a private conversation, but mobile commerce makes security even more critical – if people are going to entrust their bank account to technology, it has to be secure. [Dornan, 2001, p. 168]

Security is an important enabler for the development, adoption and the usage of the mobile and wireless technologies and services. Business, as well as consumer, applications will not be able to realize their fullest potential unless a sufficient level of trust is established in the underlying security of mobile networks.

To address current concerns the wireless product developers (including hardware and software vendors) and mobile service providers markets will have to provide end-to-end security, that goes from the user to the server and backwards. As mobile networks converge with the IP world to unified data architectures, security concerns of both areas should be viewed from an integrated perspective rather than as separate issues. The following key elements should be considered:

- Device security
- Network security
- Gateway security
- IP security
- Server security

[Müller-Veerse et al., 2001, p. 73]

Figure 12. illustrates the end-to-end security model and its components.

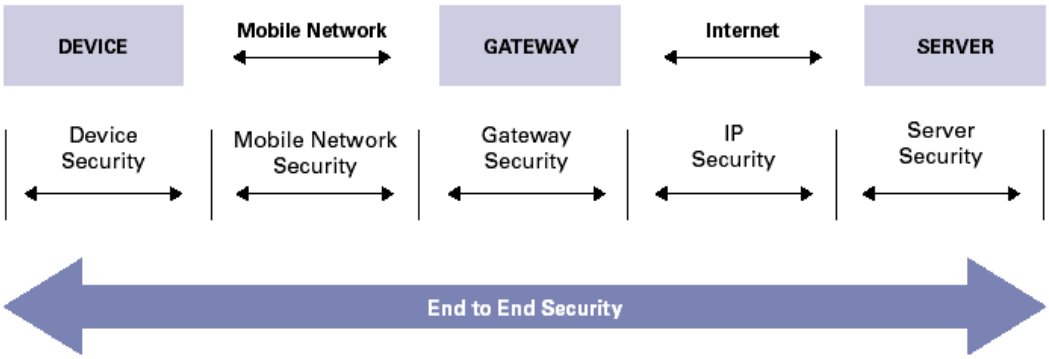


Figure 12. -to-end mobile security. [Müller-Veerse et al., 2001, p. 74]

5.5.1 Device security

Mobile devices are commonly the weakest link today in the converged data world. The diversity of standards available and their relative immaturity makes it very difficult to impose sufficient security standards on mobile device access [Müller-Veerse et al., 2001, p. 74]. The importance of the device security comes into spotlight in corporate adoption of the devices as they are becoming business tools to be used with corporate IT-infrastructure: even a robust and expensive security infrastructure may be easily penetrated through a mobile device security hole.

From devices point-of-view there are features to point out that are generally causing security problems. These are:

- As they are wireless and mobile, they can be taken almost anywhere, not just in locked corporate premises
- Typically they are small and light making them easy to lose or steal
- As the amounts of the devices is rising they are becoming a more attractive target for attackers
- Hardware features sets the limitations for certain security software to be used on the device itself (CPU, memory, battery life, etc.)
- Increasing features enable to store more confidential information on the device itself

Till recent days devices have been based on closed standards, which have meant malicious coders had to have inside information of the device operating systems to make effective attacks. Also the diversity of different mobile device operating systems has hindered the attractiveness of them to malicious coders as they had to write the code specifically for each of them. Now open standards have started to emerge in PDAs and smart phones together with new programming environments and security have gained another perspective. Just following the numbers of new viruses or attacks made during recent years show the trend towards increasing amount of them and the tendency to even more damaging attacks. Still the security problems have mainly been in the fixed world, but what if it starts to move to mobile and wireless world? Just the increasing amount of mobile devices over the more fixed desktop PCs with the other features of new devices and network, such as always-on connectivity, push capabilities of packet based networks and the emergence of multi-platform languages, will open unlimited possibilities for the propagation of malicious code, both within the mobile network and across IP networks.

Currently there is on the markets security software such as anti-virus software, file encryption software and VPN clients for Palm, Symbian and Pocket PC based PDAs from the leading security companies. Still their penetration has remained low.

5.5.2 Network security

Wireless communications use air interface to carry the electromagnetic waves that carry the information. The air interface has the security concern that anyone in the range of the communication can intercept the data being transferred through it. And it is a lot easier than intercepting communications in fixed network as the waves in the air go all over but in the fixed line they do not leak out of the cables; in the fixed world the eavesdropper has to know where the lines are going to tap to them.

Other security problem with the air interface has been the fact that the radio waves will not stop to certain borders like organization's physical premises. This is serious problem with WLAN implementations as in the cities many offices are building their own WLAN networks near to each other as one might think the possible concerns in a office building where in every floor resides a different company with its own and different WLAN. This is basically equivalent to leaving an open network connection for everybody to peruse without the need to physically plug in a cable. To a certain degree, this issue is addressed by a standard security function called Wired Equivalent Privacy (WEP). In many cases this technology alone is not sufficient, so additional security options are being developed for WLANs to enhance the protection provided by WEP [Müller-Veerse et al., 2001, p. 74].

Another problem, especially with networks within unlicensed frequency bands (e.g. IEEE 802.11b, HomeRF, Bluetooth), is that the other networks on the same frequency bands or near to each other can interfere each other's communications. Some solutions to this problem have been suggested with IEEE 802.11b and Bluetooth as limiting the frequencies used so that they will not hop on to each others frequencies. Still this does not address the problems with other outside interference sources like microwave ovens.

For data security reasons almost all wireless networks have to have some degree of network security with their own security (encrypting) algorithms or mechanisms. The degree of the security within the network without outside encrypting depends on the network. For example, GSM communication is encoded with a 128k algorithm to ensure secure wireless transport. Each of the users is assigned a temporary code that enables them to receive only the digital signal sent to them. In an eavesdropping scenario the time required to crack the code is usually longer than the life of the temporary key. The security offering capability of the upcoming UMTS system is going to be higher due to the higher data rates and more complex modulation schemes. Alternative network technologies are to a larger extent subject to security issues [Müller-Veerse et al.,

2001, p. 74]. IEEE 802.11b has been widely criticized for its lack of network security; WEP has been able to crack in just 15 minutes of listening to the network traffic and collecting the data sent across WLAN with applied software.

5.5.3 Gateway security

Gateways operate between the mobile or wireless devices and the fixed network providing the information of fixed network to the device and vice versa. In some cases the gateway also transforms the content to a form that the other end can understand it. On a higher level, communication between the device and the gateway is also subject to being protected by data security protocols [Müller-Veerse et al., 2001, p. 74]. It is also possible due to technical reasons that the wireless transfer channel and the fixed channel have different security methods as for example in Internet TCP/IP network (SSL) and in the GSM network (A5). The transforming of the information from another encrypted form to another is then done at the gateway. In the former version of WAP (1.1) this was done by first decrypting the content and then encrypting it again with the other algorithm. This left a little theoretical time space open for hackers to get the content in plaintext. In the newer release of WAP (2.0) this should have been addressed.

5.5.4 IP security

The security of a public or private IP network is a problem that is not directly related to the mobile space. Still, this is a very important component of an end-to-end mobile data security infrastructure.

At the moment, sensitive data communication is being protected by various encryption technologies. One of the basic widespread standards is SSL (Secure Socket Layer). Other standards using more sophisticated encryption schemes are also available. [Müller-Veerse et al., 2001, p. 74]

In the future, mobile traffic on the internet may be protected by a protocol called IPsec (Internet Protocol Security). It is a developing standard for security at the network or packet processing layer of network communication. IPsec will be used to create highly secure "tunnels" for mobile data in the underlying IPv6 network as all traffic moves to IP [Müller-Veerse et al., 2001, p. 74]. IPsec will be especially useful for implementing virtual private networks (VPN) and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without changes required to individual user computers [Whatis?com, 2002a].

The proliferation of mobile devices also imposes additional requirements on corporate network management. Large companies are starting to incorporate mobile device security features into their enterprise security products. Tivoli, for example, has upgraded its SecureWay Policy Director software to centralize the security management of cell phones, PDAs and other handheld devices. [Müller-Veerse et al., 2001, p. 74]

5.5.5 Server security

Server security is not directly related to the mobile security but servers are in an important position for the services and applications and very important components of an end-to-end mobile data security infrastructure. Servers might store valuable and confidential information that is not meant to be open for public. Only the individuals with permission have to be let in to access that information. Also the availability of services should be guaranteed. With increasing numbers of mobile devices hackers will be attracted to try to exploit the possibilities of doing so called denial-of-service attack, laming down a server with too many requests from millions of devices that they possibly could gain the access. Also the servers are in a key position to spread malicious code to other devices or to prevent it.

5.6 The Human Factor

Computer security is difficult, to the vendors of software and hardware products, but also to the users of those products. Even if the hardware, the software and network were secure, the complete system could still be jeopardized by one user that does not care enough about security.

Security of computers and systems always interacts with users, and as commonly the user is a human, it is the security of the interaction between human and the computer or system. One does not need to look far to find an easy example of this. One such example would be a user that prints out confidential information from a company's secure intranet and then forgets the paper to a common printer or even to an airport lounge. Even though the system was secure, the user made the information insecure by carelessly handling it.

Schneier states the reasons for this lack of security in common: people don't understand computers and people don't understand risks. [Schneier, 2000, p. 255]

The importance of security policies and rules is increasing as companies implement their mobile strategies and deploy mobile devices into business usage.

5.7 Security tools

To be able to gain security's three goals, availability, integrity and confidentiality, there are different tools. The tools of security are largely based on mathematical science (e.g. cryptography) and analysis of the content (e.g. Antivirus software).

5.7.1 Cryptography

Cryptography is the science of information security. On one level it is a bunch of complicated mathematics and on the other, it is the core technology of cyberspace,

how to make it a safer and more trustworthy place. Without cryptography e-commerce could never have become what it is today.

Cryptography includes techniques such as microdots, merging words with images, and other ways of hiding information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (encryption), then back again (decryption). [Whatis?com, 2002b]

Modern cryptography is concerned with the following four objectives:

1. *Confidentiality* (the information cannot be understood by anyone for whom it was unintended)
2. *Integrity* (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3. *Non-repudiation* (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4. *Authentication* (the sender and the receiver can confirm each other's identity and the origin/destination of the information)

[Whatis?com, 2002b]

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders. [Whatis?com, 2002b]

Encryption and decryption methods used for different algorithms are based either on symmetric encryption, asymmetric encryption (also known as *public key cryptography*) or one-way hash functions. Also these methods can be used combined for performance reasons. Asymmetric encryption is rarely used alone as

it requires more computing power and so it is often used with symmetric encryption; the content itself is encrypted symmetric (same key to encrypt and decrypt) but the symmetric key is encrypted asymmetric. The symmetric key is typically a *session* key, a key created randomly out of thin air.

As cryptography is based on mathematics there are still methods of breaking the encryption algorithms and the messages encrypted. Brute-force attack is the simplest but the longest way of breaking an encrypted message by calculating every possible key to open the message. Today's best algorithms used with strong and lengthy enough keys (currently standard being 128 bits) still make the breaking with brute-force method a hopeless act as the computation of all the possible keys could take millions of years even with the most modern and the most powerful computer. The increase of computation power of a single computer (like Moore's law expects it to double every 18 Months) decreases the time, more effective attacks to break encrypted messages by networking computers through Internet.

5.7.2 Authentication

Authentication is about the continuity of relationships, knowing who to trust and who not to trust, making sense of a complex world [Schneier, 2000, pp. 68-69]. People authenticate themselves many times a day, even without recognizing it, but it is still one important part of our daily lives; recognizing the faces, voices or other recognizable features of our trusted partners, colleagues, relatives or even goods or services.

In information technology, authentication is still mostly seen on usernames and passwords when signing on to a computer, network or a service. Many times these usernames are easy to guess from user's real name and then the security depends on the password and its strength; how difficult it is for unauthorized people to guess. Username and password combinations can also lead to false sense of security as some of them are even easily breakable and even in the Internet there

are guides to bypass some of username and password authenticated systems. A bit safer method of authentication would be to use a physical token, such as a smart card, and a password combination, as without the token it would be impossible to sign in to a system even when knowing the password or so called PIN (Personal Identification Number).

To make authentication more secure in electronic world, cryptography is widely used to create authentication keys. Mostly are used the keys based on Public Key Infrastructure (PKI), where asymmetric cryptography is used to create a key pair; one public key can be published for all the others and the other private, only known by the user. Normally the key pair is used to send messages encrypted with the receivers public key, so only the receiver can open it with the private key. In the authentication the key pair can be used otherwise; the user crypts the message with his or her private key and the others can verify that the message was from the sender, not from another person, by decrypting the message with the sender's public key.

Digital signatures, credentials and certificates, are also used for authentication purposes. There are several digital signature algorithms in use currently, RSA being the most popular.

5.7.3 Virtual Private Network

Virtual Private Network (VPN) connects computers, which can be located around the globe, to a private network using public networks. A VPN is a 'virtual network' since connections are established only on a when-needed basis. The transmitted information is encrypted and tunneled point-to-point over a packet-switched insecure network. At the receiving end, the information is decrypted, filtered if necessary, and checked for integrity. A VPN provides network users with an inexpensive, safe and scalable security solution [Intel].

VPN can be implemented in several ways and in different levels. It can be implemented between two local area networks (LAN-to-LAN), from remote user to local area network or within an intranet [Intel]. The levels of VPN vary from the simplest, when the VPN encryption covers only the tunnel over the public network between the servers, to the highest(the most advanced), the end-to-end VPN encryption tunnel which starts from the user's device and ends to the other end, server or other user's device and the content transferred is always encrypted independent of the network it goes through. Figure 13. illustrates a virtual private network connection from mobile device

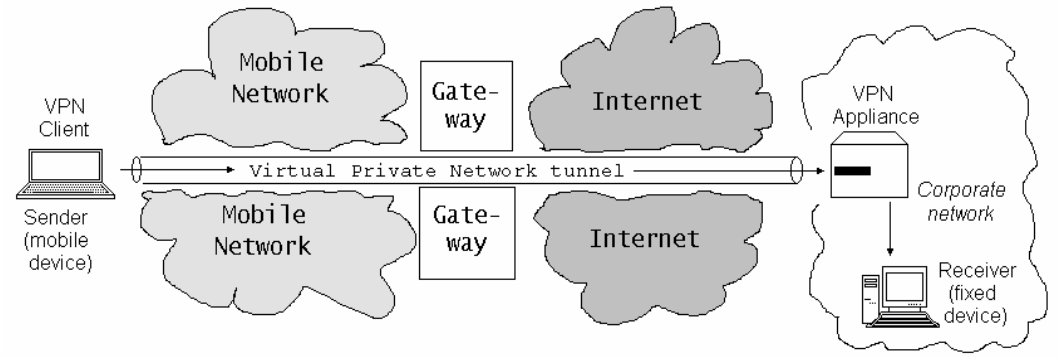


Figure 13. Virtual Private Network between mobile device and corporate network. [Adapted from Intel, 2002]

5.7.4 Firewall

Firewalls have generally been used to separate corporate intranets from the Internet by providing access control. A properly configured firewall prevents unauthorized access to or from private networks, especially Intranets. All messages (i.e. all IP traffic) entering or leaving the Intranet pass through the firewall, which examines each message and blocks messages that do not meet the specified security criteria. A Firewall is one of the fundamental components of a secure network.

Functions of a firewall can include:

- The firewall examines each packet entering or leaving the network and accepts or rejects it based on a predetermined list of criteria.
- The firewall provides an applications gateway that can apply security mechanisms to applications such a FTP (File Transfer Protocol) or Telnet servers.
- Circuit-level gateways apply security when a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) connection is established.
- A proxy server intercepts all messages entering and leaving the network, while hiding the true network address.

[Intel, 2002]

Firewalls can be hardware or software based. Hardware based solutions are often designed for large scale IP traffic such as large corporation intranets. Software based firewalls are designed for smaller IP traffic, such as even single computers. In the age of powerful viruses and worms and always-on connectivity it is also recommendable to have a software based firewall on a single computer to prevent unauthorized access and usage of that computer, even a handheld.

5.7.5 Antivirus software

Antivirus software is a program that detects malicious code, such as computer viruses, worms and Trojans and tries to prevent them from execution. There are three kinds of antivirus software; active, passive and combined. Most of the current desktop versions are combined: they include the active part that constantly seeks for malicious code in the working memory of the device and also have the user initiated passive search for malicious code of hard drives or removable medium such as floppies and CD-ROMs. For mobile devices there are still many passive only antiviruses as many of the mobile devices are short on computation power. For the search for malicious code the device itself is then typically brought

near to a desktop computer that then checks the mobile device's memory. The lack of active antivirus software on a mobile device makes it reasonable to use active antivirus on the gateways and servers used for mobile devices.

In desktop computing world, or let's say Windows based world, the last few years have seen the huge increase of viruses, worms and Trojans spreading through the Internet. At the same time the destructiveness of them has increased exponentially. In the wireless world this has not yet happened as the operating systems of mobile phones have been closed and there is not such a monopoly in operating systems of the other mobile devices, such as PDAs. This is surely about to change when the device numbers are increasing and the battle over the operating systems has led to two main stream operating systems in maybe three years time. Then the device numbers are enough to attract more and more writers of such viral code, even just for publicity. To date there have only been few viruses for mobile operating systems such as Pocket PC, Symbian OS and Palm OS.

5.8 Security as investment

Security is an important enabler for doing business. That is why it is easy to see companies invest even large sums of money and time to have even more secure systems. But as Bruce Schneier says it: security is a process, not a product. You just can not buy a box of security out of the shop; it is the whole philosophy how the things are done, how all the components are dealt with. It does not help if you buy firewall software from a store, but can not use it.

As companies invest in their security - security products, usage and education – they have to consider the costs versus the size and nature of the business. It has been said that the data is worth protecting only by its value. This means that there is no reason to spend a million Euros to secure just one Euro transaction. Also many times in business it is enough that the data or information is kept confidential for some months or years. Then it is only reasonable to use methods that keep it safe for that required time.

Absolute security is maybe impossible to create as the evolution of technology goes on and makes old technologies and techniques obsolete. The more secure system you want, the more you have to pay for it. Still more important is the balance between the security level and the cost.

6 MANAGEMENT OF WIRELESS TECHNOLOGIES

This chapter discusses the technologies, services and security depicted in earlier chapters and combines them into a managerial portfolio point of view – how they relate to each other and what are the challenges in a corporate adoption of wireless technologies and services and what has to be considered when implementing wireless technologies.

6.1 Acronyms used in this chapter

HMSP	Horizontal Management Services Provider
ASP	Application Service Provider
MASP	Mobile Application Service Provider

6.2 Managing mobility

Although the business world is increasingly mobile, many corporations are resisting the idea of wireless communication, because of concerns about set-up and maintenance costs and the need for so called in-house expertise.

A recent study found that some companies that have invested in web-enabled handheld devices for use by field personnel have struggled with specific applications. Without effective middleware integration, mobile access to back-end enterprise systems, such as databases, can be too tedious for busy frontline employees. These organizations are learning the hard way that the desktop paradigm does not always translate smoothly into a handheld environment. [Davies, 2001, p. 38]

A major challenge to the implementation of a mobile workplace is to change the corporate mindset – the top management has to be convinced that people can be more productive if they have easy access from anywhere they are to corporate data and information.

6.3 Management areas

6.3.1 Managing networks

Managing network access in a company is mainly considered as managing the own corporate LAN or intranet and the elements belonging to it as well as managing the connections to and from other networks.

When wireless network access scenarios are added, network management will also cover the service agreements with operators of other than corporate network and the management of access from those networks to corporate networks. As the user travels through different areas, corporate premises, urban and rural areas, he or she might have different wireless access technologies (networks) at hand in different locations. Still as the user moves from another area to another he or she should be able to have the next possible access technology in use with an access device (terminal) requiring only minimal effort to change the settings for the new network environment. Figure 14. illustrates the possible network schemes. In the office an employee can use the Personal Area Network (PAN) by using Bluetooth or infrared access. When moving to other corporate premises or some public places that have WLAN, the user is automatically handed over to WLAN network. As the user enters the world outside the WLAN networks but still stays in areas where UMTS networks are in use, he or she is handed over to the UMTS network. In rural areas where no UMTS networks are deployed, the user will be handed over to the GPRS or EDGE network.

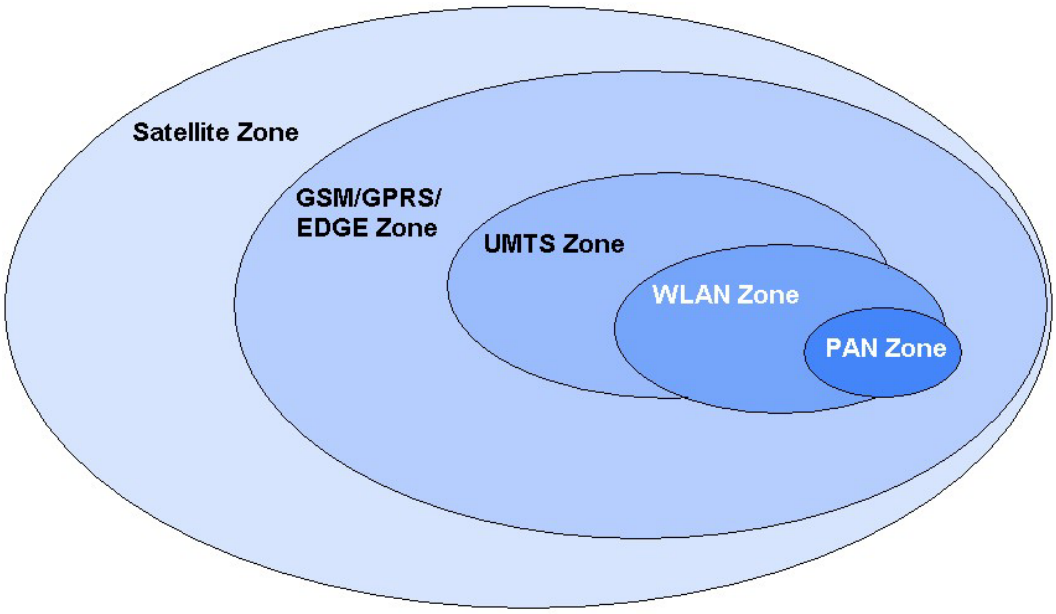


Figure 14. Multi network environment [Adapted from Müller-Veerse et al., 2001, p. 58]

The terms of roaming and handover have been used in an ambiguous manner. The term roaming is usually reserved for using a phone on a network owned by a different operator, usually in another country. The process of switching a user from one cell to another while the call is in progress is called a handoff, or handover [Dornan, 2001, p. 47]. As voice concentrated services are moving to data centric ones these terms are also used in data centric networks. Handover is also used when a user switches from one access technology to another that is operated by the same operator, e.g. from WLAN to UMTS or GPRS.

Currently the devices themselves are rarely functioning in multi network environment. There is still need for different external cards, such as PC cards, for almost every different access technology. In the near future there will be multi network functioning PC cards, such that have at least two different access technologies integrated into one card, e.g. WLAN and GPRS. WLAN is also predicted to be integrated into laptop computers in the near future, but nevertheless, there is the problem of deciding which of the several WLAN technologies that will be. Also it is predicted that in the near future mobile so

called dual mode phones are capable of operating in GPRS/EDGE and UMTS environments.

The handover or roaming between the networks is not easy yet as everyone of them needs characteristic configurations to the devices. These are the major problems that technology developers must overcome to make it easier for the users.

Another thing to manage with the access technologies is the availability. As in high traffic areas the network congestion is the problem, the users should have another option (access technology) available in case of urgent data transfer needs.

6.3.2 Managing terminals

Terminal management is maybe the most challenging part to manage. Even if the company would have the same equipment (or at least the same operating system in the mobile devices) with every mobile worker the equipment itself is not the only problem IT-managers have to encounter. As the terminals are developing and getting even more features and capabilities through software, the management challenge of the software on mobile workers' devices will increase exponentially with every new software or application and also with every new user.

The software or application management involves also keeping the applications and software on the terminals of the mobile workers up to date, most importantly the security software like anti-virus software.

Another important thing in terminal management point of view is the recovery of lost information and replacement of lost, stolen or broken device. Mobile devices can currently store a lot of vital information to the owner of the device for his or her daily tasks, personal and corporate. Especially in service, transportation and sales use, there is a vast amount of critical data in smart terminals [Novo, STM]. Even in the case of loosing that information, what ever the reason is, it should be recoverable to a certain extend. One solution for that could be a network server

where the files of the mobile device will be automatically backed up when the device is within the network.

6.3.3 Managing services

The services can be the services the company itself offers to its mobile users, such as applications and information services, or third party services offered by other service providers

As a company offers services to its mobile workers it has to make sure that the different device types and network options used by the workers are supported by the company servers and gateways. The servers and gateways have to be able to communicate with the mobile devices how the information can be interpreted on the mobile device. At the moment there are few middleware solutions to cover this. Using middleware solutions a company can use the legacy systems, such as databases, SCM and CRM applications, with even newer mobile devices in the future. Most of the current middleware solutions are based on XML (eXtensible Markup Language) changing the old formats from data to XML which can then be easily reformed suitable for different kinds of terminals.

6.3.4 Managing security

Security is one important enabler for business and so the proper implementation and management of it in a mobile enterprise is evident. Managing security takes into account the whole infrastructure of the company and its workers, not just the technology itself.

One important part of security management is the creation of company security guidelines. They are then the rules by which every employee must abide. The guidelines must also follow the rules according to which those guilty of breaking them are being punished. As important as the guidelines themselves is to inform and educate employees to obey them. When these steps have been taken it is the corporate IT's responsibility to keep the infrastructure up to date.

6.4 Complexity block diagram of access management

The elements of the wireless management can be put into different tables where every new element line increases the size of the table with one line or column. As the management of technologies and access services include mainly three elements, access provider (operators), access technology (network type) and the access device, the complexity of the management of just the access will be increased in volume when one element line is added. Figure 15. illustrates the volume with four access providers, seven access technologies and six access devices.

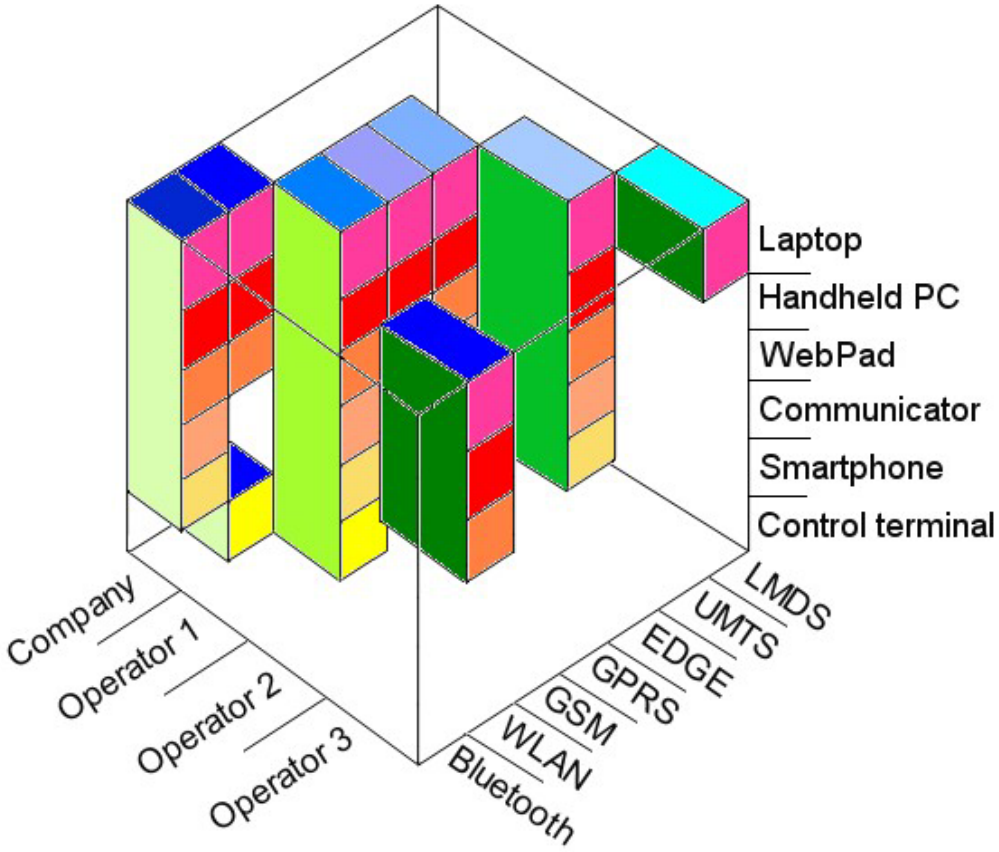


Figure 15. 3D block diagram of access management with 6 devices, 7 technologies and 4 operators.

In the figure the company itself manages the devices in Bluetooth and WLAN networks. Operator 1 is used for GSM, GPRS and EDGE services. UMTS access

is provided by Operator 2. Operator 3 offers LMDS access as well as WLAN access outside the company's premises. In the figure blue shaded colours represent the access technologies (networks), green shaded colour represent different access providers (operators) and red shaded colours represent access devices (terminals).

As currently almost all the access methods need their own configuration, the more different access types there are the more complex they are to manage. This is where the horizontal management service scenarios, provided in the former chapter, would help a company to decrease the volume of the complexity by decreasing operator count to two: the company itself and horizontal management service provider (HMSP). HMSP would then provide through the contracted operators the access to their networks and would provide the company with the settings and configurations for different access device types.

Also different access providers, operators, can use this kind of block diagram to determine their service offerings against competitors. Offered applications and services can be added to access technology axis next to different networks.

The complexity of managing other important elements than security and the applications adds easily another half to the management issues. Even though there were certain services offered, including security, some of them are still to be managed internally within the company.

6.5 Management solutions

Many companies are confronting the question of doing it self or to outsource when it comes to areas that are not in their core businesses. Complex new technologies and their implementation is certainly one of those to think about; how to handle them.

6.5.1 Doing it-self

In the doing it-self approach the company builds the mobile extension to its corporate IT services on its own. In building and managing the mobile extension the company needs to bind its IT resources and may need to use consultant services or new recruits that have the needed skills. For smaller companies or companies with a more limited IT department the do-it-yourself approach can become a too high obstacle to climb over. Larger companies generally have better resources to build their own mobile extensions as they have more funding, better IT resources and even experience on IT projects.

6.5.2 Outsourcing

The idea of outsourcing is to acquire products or services that do not belong to the core competencies of a company from outside suppliers. The reasons are many times the cost efficiency the provider can offer or the abilities that the company itself does not have to make it on its own.

The outsourcing of information technology related services has seen the rise in recent years as the technology evolution's rapid developments and the abilities of companies to keep up with the development has swallowed more and more resources. Through outsourcing of IT services companies have been able to concentrate on their own businesses and core competencies without investing too heavily on skilful in-house IT professionals.

One outsourcing solution that has emerged is so called application service providers (ASP) and its mobile transformation MASP. ASP is a company that offers individuals or enterprises access over the Internet to applications and related services that would otherwise have to be located in their own personal or corporate computers [Whatis?com, ASP]. In ASP model the applications are placed to a special application server, which can be then managed centrally.

Applications served through ASP may include:

- remote access serving for the users of an enterprise
- An off-premises local area network to which mobile users can be connected, with a common file server
- Basic office tools such as word processor, spreadsheets, presentation tools, calendar, contacts and email
- Specialized applications that would be expensive to install and maintain within your own company or on your own computer

An MASP performs the same service for wireless and fixed mobile clients as a regular ASP does for wired only clients. The main difference between the two is that MASP also enables customers to access the service from a variety of wireless devices, such as a smartphone or PDA and not only PC based devices, such as laptops and desktops.

MASPs offer businesses the advantages of wireless and mobile services with less expenses and fewer risks. Because mobile applications are subscribed to, rather than purchased, up-front costs are lower; because the MASP provides support, staffing and training costs are lower.

In addition to ASP services MASP services may include:

- Constant system monitoring
- Diagnostics and resolution
- User support
- Text and layout formatting for various devices
- Problem detection and reporting

Even though there are still some issues to be resolved, MASP provides an easier and safer option for organizations to add a mobile component to their IT infrastructure. Concerns might be confronted with data synchronization among devices and with coverage areas as they might be limited to wireless connections.

Currently there is a large number of ASPs that can offer mobility to some degree. Truly wireless enabled MASPs exist already to a certain extent and the numbers are expected to increase significantly as the adoption of wireless services and applications increases in the next few years. Still there are only few full services for analysing, planning, implementation and management of wireless terminals. Many of the wireless undertakings of the organizations are still carried out as projects with help of IT experts, such as IT consulting companies.

7 CASE: MOBILE SALES PERSON

The aim of this chapter is to provide the reader with a good picture of how the technologies and services presented in the previous chapters are combined into a real life application; the needs for technology and services, and the limitations they might have.

7.1 Execution of case study

The case example is chosen to demonstrate a not so uncommon example of utilization of wireless technologies and services: a mobile sales person who needs mobile tools to execute his daily tasks.

First it will be viewed what the common challenges are in implementing wireless solutions. Next we will view the requirements for the tools set to make the sales person mobile; what the sales person needs and what is there to gain.

Later the requirements and needs will be put into perspective with the former chapters (technology, services, security and management). In the end there will be discussion and conclusions of the case.

7.2 Common challenges of wireless mobile solutions

The common challenges of wireless solutions can be classified as following:

1. Usability
2. Network security
3. (Un)reliable networks
4. Scalability
5. Enterprise integration
6. Extensibility

[Vaultus, 2001]

7.2.1 Usability

The first challenge is to make the applications easy to use and at the same time allow consistent, always available access to relevant data, even when network coverage is not available. For the sales persons this would mean that they had the most important and mission critical data for their daily tasks on the device itself they use. That data could then be updated from corporate servers and databases when the network connection would be available and at the same time the new information written while offline would be backed up to a corporate server. Also the basic applications would have to be installed locally to the device itself to make them useful when network access is not possible.

7.2.2 Network security

The second challenge is the network security. The data sent and received should never be exposed en route between the user and the corporate firewall even when using different networks and technologies. Only a VPN solution provides a truly network independent solution as different wireless network technologies have their own distinctive security features and characteristics and vary from insecure to almost secure. For extremely confidential information the security of wireless networks is not enough without network independent solutions like VPN. Also the security should be enforceable from a central, administrative console to ensure compliance.

7.2.3 Unreliable networks

The third challenge to overcome is the network reliability. The lack of high-speed and robust wireless networks necessitates a mobile application solution that minimizes network reliance, optimises data transport, and mitigates the disruption from dropped connections. For the design of the applications this means that the

most critical information exchanges should be designed to be carried out in the narrowest band network used for the application and that only the most critical information is transferred. Disruptions and errors can be handled by applying techniques to ensure the integrity of the data transferred.

7.2.4 Scalability

The fourth challenge is scalability. The proliferation of wireless devices and mobile applications creates an immense administrative burden on corporations. To attain their full return on investment, even large-scale solutions must be completely and easily manageable by just few centrally-located administrators. For these management and also security reasons it is reasonable and recommendable to separate corporate mobile users to a separate sub network with their own firewall and servers. To cut down the amount of wasted time it is also important that the users could update their user profile, device profile, or mobile application suite on the road without having to return to the office. All the necessary updates and data synchronisation should be able to be done on-the-air as requested as the device is connected to the network. Security updates would have to be forced so that the users could not avoid them. This way also a stolen or lost device could be locked up as it enters a network.

7.2.5 Enterprise integration

The fifth challenge is to integrate the mobile applications to existing enterprise systems. Mobile applications must be able to access all relevant corporate data and still fit seamlessly into existing corporate infrastructures. Enterprise legacy systems and databases are adaptable to new forms by using middleware solutions: the information on old databases can be converted to XML format, which is then easier to refine and reform to other forms. Middleware can also be used to recognize the user's (mobile) device and its capabilities and then reform the data into a form the device can understand. The same thing can also be done vice versa

when the user sends information back to database from the device. This is called adaptive infrastructure.

7.2.6 Extensibility

The sixth challenge in wireless applications is the extensibility. Solutions or applications should be adaptable to changing needs: they should be able to evolve as business needs to evolve. Extensibility is best achieved by applying open standards. Currently Java is fast becoming as a standard in mobile computing and mobile applications.

7.3 Effects of mobility

The effects of the mobility in a company can be seen as in the figure 16. In the middle of the figure are the company's premises – "In-house". The outer parts consist of the company's partners, customers and outside world. The four arrows depict the effects when moving across the environments. First arrow depicts the potential users of the mobile applications which increase when moving outside of the company's premises. The second arrow depicts the real-time information supply that increases when moving outwards as for example the sales personnel gain new information from the customers as they make the orders and input them into company's systems.

On the downside the third arrow depicts the decreasing access opportunities when moving out of the office, as in the office there are possibly access to different network technologies (e.g. Bluetooth, WLAN, fixed Ethernet, etc.) but at the customers side the mobile network (e.g. GSM) might be the only choice available. The last arrow depicts the decreasing features when moving outwards. In the office all the applications and services are available in the office networks as bandwidth of the networks are broad enough, but as in the country side the narrowband mobile networks may be the only solution to use, all the applications and services might not be available.

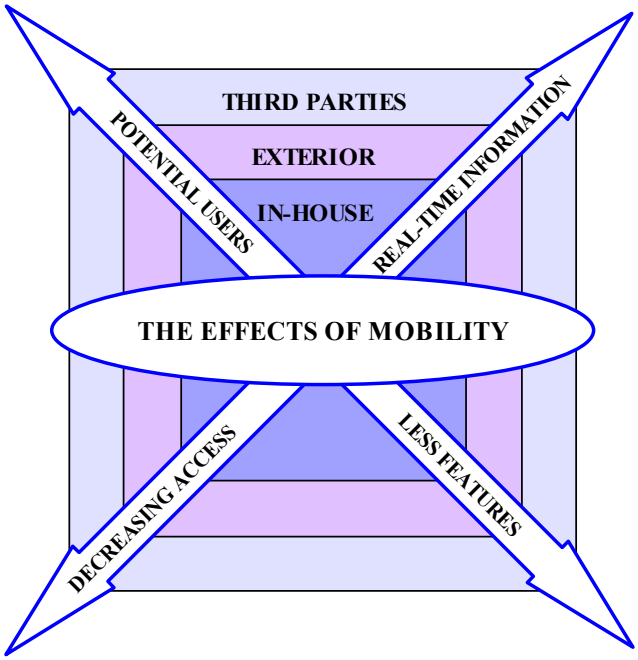


Figure 16. The effects of mobility.

7.4 Demands for the wireless mobile office

Mobile sales manager sets a certain set of demands for the technology and services to make him/her to be able to carry out his/her daily tasks around the globe, independent of time and place. It is a lot more efficient to put sales personnel out chasing after customers than to keep them in the office waiting for the customers to call them.

The sales person on the road needs the same set of tools he/she might have on his/her usage in the office: network access, access to the company's information and data bases, software tools for communication (email, voice calls, fax, etc.) also when driving a car, notes and reports, presentations and time management (calendar). The mobile sales person should have the same set of services available as he/she has in the office, also with almost the same usability and speed; as if he/she had a "wireless mobile office" in a briefcase.

The benefits for the company would be better information, decreased time for response and more sales (more commissions).

7.5 Terminal requirements

The requirements set for wireless mobile office propose the requirements for the terminal as the following:

- having the capabilities at least near to a desktop computer in a briefcase or even smaller size
- capable of handling all the basic office tools (i.e. word processor, spreadsheet, presentation tools, data base tools, time management, etc.)
- the device should be able of handling emails, voice calls, faxes and possibly instant messages
- for communication purposes the device should be able to be connected to different kinds of networks (GSM/GPRS, UMTS, WLAN, Bluetooth, etc.) through integrated radio components or via extension cards

Possible other requirements could include:

- easy and fast start up (fast and flexible usage)
- always-on connectivity

Due to the requirements the terminal could be a device ranging from a communicator to a laptop PC, depending on the preferences and display size needs of the user. A communicator, e.g. Nokia Communicator 9210, has the basic tools for office applications (word, spreadsheet, presentations, calendar, web browser, email, fax and voice calls) and other applications can be written on its Symbian OS operating system. Limitations for Nokia 9210 are its connectivity to other wireless networks; the only radio frequency network it is connectable is GSM (HSCSD) networks. It also has a possibility for an infrared connection to other devices, such as digital cameras and other PDAs. Future communicators

include Bluetooth connectivity integrated and at least GPRS, EDGE or UMTS public network connections to offer speedier data transfer. Also the pocket size display could make some limitations in usability.

Palm top and handheld computers have often the same basic applications (word, spreadsheet, calendar, web browser, email, etc.) as communicators but are also more flexible with different network connections. Palm top and handheld computers commonly have extension modules or integrated slots for PC cards, which then can be used to make them connectable to different networks, also making voice calls with them possible. Also in these the size of displays may have some usability limitations, e.g. viewing larger spreadsheets.

A third possible category of devices includes tablet and laptop PCs, which already offer the same software and application range as a typical desktop PC in the office making the same files directly usable in the office and on the road. Tablet and laptop PCs have the connectivity to radio frequency networks often through PC cards, but possibly in the future some of the technologies (e.g. Bluetooth and WLAN) will be integrated into them. As tablet and laptop PCs are based on the PC standards, they also contain the same basic components as desktop PCs, like hard drives offering more storage capacity for files, and powerful processor giving the power for more demanding applications than the smaller competitors can handle. Tablet and laptop PCs have full size displays to make it convenient to use and view web pages, spreadsheets, and presentations. Due to the full size display they might be clumsy in situations where also a smaller pocket size device could do the job. Due to the powerful features and complexity the prices for tablet and laptop PCs are easily double or even more compared to the pocket sized devices.

To specifically select the terminals for the “road warriors” it is important to compile the list of absolutely needed features, preferred features and not wanted features. In one device it is not possible to have all the wanted features, so there is always need for a compromise in the selection of the appropriate device or devices.

7.6 Network and network access requirements

The requirements for the networks and network access can be defined as:

- Easy roaming between different networks and network technologies (GSM/GPRS/EDGE/UMTS/WLAN/satellite/etc.)
- Access to networks is global
- Transfer speeds should provide near the same usability and flexibility as in fixed office
- Networks should allow transferring speech and data, both simultaneously

Roaming or handover capabilities of current networks and technologies still leave much to hope for. Different technologies are available only through different extension cards which may require some configuration when changed to other networks. Device integrated multi network features are yet to come. Also there are only few roaming agreements of the operators with different wireless network technologies; even within GPRS technology the number of roaming agreements was at the beginning of 2002 still quite low compared to the number of GPRS networks built to that date.

Only truly global access is provided through satellites. Still currently operated satellite services provide only narrowband transfers up to some tens of kilobits per second. Other limitation of satellite connections is that they function only in "open-air" and may not be used inside the buildings. The paths of different mobile networks in different parts of the world have also their implications for the selection of the network services. Continentally the network options are more homogenous, e.g. GSM in Europe.

Data transfer speeds of different access technologies vary from very narrowband to broadband. Current mobile phone networks support transfer rates up to some

tens of kilobit per second, HSCSD up to 57,6 kbps and GPRS up to 53,6 kbps. Still GPRS has had many technical problems and seems that the normal speeds stay just above GSM Data, 10 – 20 kbps [DigiToday, 2002]. Also the predicted 2 Mbps of UMTS seems far from real at the beginning of the services. It will be more like ranging from some tens of kilobits per second to some hundreds. Figure 17. illustrates the expected real transfer rates of mobile phone networks between the years 2000 and 2005.

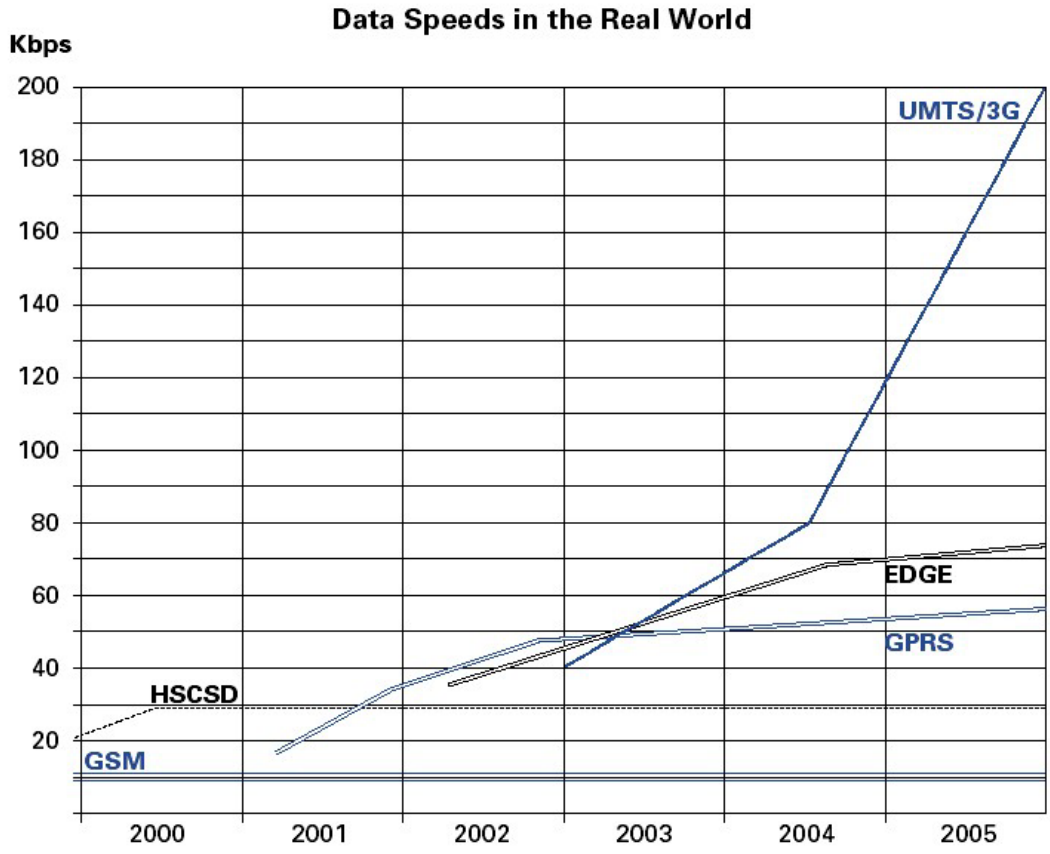


Figure 17. Real world data speeds. [Müller-Veerse et al., 2001, p. 53]

More important change than the increase of transfer rates for the applications is the change to packet switched and IP based networks. They present the always-on possibility and shortened response times when connected. Also the billing from services in packet based networks allow different kinds of approaches than in circuit switched and for applications, such as email, that do not require constant connections packet switched networks are more favourable. The applications, or

the content, will not be as fast through the mobile networks but almost as convenient (depending on used device) as in office surroundings. Only wireless LANs, such as IEEE 802.11b, can compete today with a normal office surrounding in terms of transfer speeds, as they can deliver it up to 11 Mbps.

The request of transferring simultaneously data and speech is only possible in true IP networks. In today's mobile networks, GSM or GPRS, it is not possible. In GSM only one call at a time is possible, whether it is a data or speech call. In GPRS the data connection will be put on hold as speech call is received. Wireless LANs are capable of transferring data and speech simultaneously, as the speech will be transferred through Voice over IP (VoIP) to another computer or phone. To make a call to telephone networks, normally a special service and an account for billing are needed when making such calls using VoIP.

7.7 Service requirements

The services the mobile sales person would need on the road could be categorized in two classes. The first class of the services would include those applications that the company could offer for the mobile sales person. Those services would consist of the mobile intranet access, corporate email, contacts and calendar as well as the enterprise systems, such as databases, ERP, SCM and CRM. The second class would be the services acquired from other service providers, such as operators, content providers and ASPs. Those services would consist of basic data and voice transfer capabilities, Internet surfing, information and news services, messaging services as well as possibly location based services. Messaging services should consist everywhere of at least the basic voice calls and SMS or MMS messages. More flexibility good be brought by implementing VoiceXML services, which the sales person could use for example to read the mail by listening while on the move or order plane tickets from the service with the help of it.

The corporate services as well as the other services should be enabled on a 24/7 basis, meaning 24 hours a day and seven days a week as the mobile sales person

could operate globally. Services should also include backup tools for critical data that is stored locally on the sales person's device as well as synchronization tools for important files that normally reside on the corporate intranet but are constantly needed by the sales person.

7.8 Security requirements

As the sales persons of a company may have confidential information of the company and maybe of its partners stored on their devices, that information should be kept confidential and protected against unauthorized use. The security of that information should be at least on the same level as it is inside the corporate intranet.

To achieve the level of security of corporate intranet firstly the unauthorized use of the device should be made as much impossible as possible. This requires authentication methods to be used, such as PINs or passwords. More recommendable would be the use of a physical token, such as a smart card or an electronic key placed into USB port of the device, with a password if possible. Some of the bigger devices, such as laptops and handhelds support them, but smaller devices may be more problematic. Later when the single sign-on services are reliable, they also could be used for authentication purposes to get rid of the hassle with many passwords for different services. The authentication could be made when the person accesses the corporate intranet.

Second important point to improve security is that all the data stored on the device should be encrypted to prevent the data ending up in wrong hands in case of property theft. Thirdly, all the data communications between the device and corporate intranet should be secured network independently for example with VPN technology. Currently there is available VPN client software as well as file encryption software for the major mobile device operating systems. Fourthly, in case of loss or theft of the device it should be able to lock up to prevent

unauthorized usage. This may not be fully possible globally, but at least the connections to corporate intranet are possible to be prevented from further losses.

7.9 Management requirements

Management of the devices, services (applications) and security posses a challenge to corporate IT. The more components there are in the mix the harder it is to manage. Whereas mobile and wireless devices are desirable, at the same time the corporate services (applications) would be centrally manageable. If the whole mobile extension of the company could be centrally managed, the security would also be easier to control.

The corporate services to mobile extension can be offered through specific corporate platform that is configured to deliver data between other corporate infrastructure and the mobile device. The whole mobile extension is recommendable to separate to its own subnetwork within the corporate network. All the data between the fixed corporate network and the mobile corporate network goes then through a specific firewall to guarantee data security. Unauthorized requests and attempts through the mobile subnetwork to the fixed corporate network will be blocked by the firewall. In the mobile subnetwork servers could be used as middleware solutions to reform the data sent to the mobile device that it is fitted into the right form and the right layout that the device can understand. The same is then used vice versa when data is sent from the mobile device to corporate systems. This is called adaptive infrastructure.

7.10 Discussion and recommendations

The case of a mobile sales person shows how much different points of views there are to consider when a company decides how to implement it. Even though the case is not based on fully specified needs and requirements, analysing of the basic needs from the side of the sales person as well as from the side of the company leads to many rising questions.

On the one hand the sales person wishes all possible that could help him or her to do the daily tasks as flexibly as possible and hopes for the best possible tools. On the other hand, the company requires the most secure the easiest and the most cost efficient manageability possible of the mobile extension. Most possibly, and also advisably, the compromises are made at the expense of the flexibility and feature richness of the device and services side for the sake of security and manageability.

Before an organization starts to plan its mobile extension for the sales personnel and/or the executives, it must define all its needs and requirements very specifically. That is, a detailed account in every aspect of what is needed and how. After that it should be analysed what the organization's own possibilities are to build and manage it and compare it to other possibilities to build and manage it.

As there are currently hundreds of different kinds of terminals alone, without any more specific details of the mobile sales person's applications, corporate systems or the needs of specific sales persons, this is not the place to make further and more specified recommendations, as one organization is not the same as another. The same applies to the needs and requirements as they can vary considerably in different organizations.

7.11 Conclusions

Mobile sales personnel are certainly among the first adopters of the benefits from wireless technologies and the mobility and the flexibility they can offer for the daily work on the road. All the needed technologies are already available to build such a mobile extension for sales personnel that they can do their daily work on the road as if they were in the office. New technologies and open standards will open up new possibilities to implement tools for mobile sales personnel in many different ways with different device and network combinations. Still, the attention must be paid to security and management concerns; sales personnel are also the representatives of the company. The image of how things are handled in the

company may be showing out to the customers also through the reliability of the equipment and systems in the hands of the sales person.

8 DISCUSSION AND ANALYSIS

This chapter ties together the earlier chapters and the experiences of the writer from the time spent on doing this study. The situation with wireless technologies, services, security, managing and all this together will be discussed analytically and some future visions will be reviewed. In the end there will be a discussion about this study and further points to study will be suggested.

8.1 Wireless today

Second generation mobile phone networks are reaching their evolution peak as the technology, or so to say, the spectrum used in second generation networks is reaching its limits. Ever increasing capacity or bandwidth needs are driving the need for new technologies such as third and fourth generation mobile networks. However, there is still a long way even for the second generation networks before they have exploited their full potential as third generation networks are just taking their first step in commercialization. Already now with GPRS packet switched networks it is possible to offer services and applications that are just getting better when the third generation networks offer more bandwidth for their use.

Companies are also keen to watch out for other wireless technologies to transfer data than the operator oriented technologies. The reason is purely high costs of currently operated networks for ever increasing bandwidth needs of companies. Also other benefits, such as flexibility and cost efficiency, of the wireless networks have been drivers for Wireless LANs. There are plenty of corporate applications, such as warehouse and fleet management, and personnel, such as travelling executives, mobile sales force and maintenance, which can benefit from wireless technologies. Still, the biggest problem seems to be that companies themselves have not made clear what they expect from wireless technologies, where they would need them most and what the benefits are. It has come up in several articles and interviews that in many companies wireless technologies and services have been seen just as costs, whereas the real benefits have not been seen.

Many of those benefits cannot be directly counted in money. Such benefits can be for example the avoidance of stress, and due to less sick leaves of the personnel.

8.2 Current status of wireless elements

8.2.1 Terminals

Mobile small terminals, such as PDAs, aren't yet suited for business critical applications and stand alone products. They still need a PC (desktop or laptop) for data back up and for storing data longer as few weeks or months. Small handheld and palm top computers are still good tools for messaging, acute information pick up, making quick notes and personal information managing, but lack the capabilities for rougher applications due to display and data storage limitations. Also many of the current PDAs lack important security and back up features to make them real business tools.

The problems with PDAs and their usability and security lacks originate in many cases from the world of desktop computers as the manufacturers have tried to adopt almost everything possible in features from them to a miniature size without paying attention to reliability, usability and security matters. Reliability in this context is how the data is stored in case of power failures or when batteries run out of power. Other PDAs that come from the mobile phone side have often less features but instead are more reliable and usability is better than in the devices from PC side as the battery life and power consumption is better handled as well as the way the data is stored in case of loss of power. Both sides are closing up on each other but before the computer industry has solved the usability and other critical problems, PDAs that come from the mobile industry side are to beat them in critical usage as the conditions normally are in business usage.

Laptop PCs will certainly remain the main tools for mobile personnel for some years as they offer the full fledged features and the performance of a desktop computer. As the size of laptops may not get any smaller the performance and features will still increase. In recent years so called subnotebooks have entered the

market. These are laptops without integrated peripherals like floppy or CD-ROM drive to make them smaller and lighter. Also the lack of corporate standards for PDA type of devices may hinder the adoption to corporate usage. Also the amounts of different kind of PDA products and the fast pace of technological development may put companies “on hold” to wait for newer and more advanced products. As now there are hundreds of different wireless terminals and tens of different types of them on the market, the next few years will show the terminal types that will survive.

8.2.2 Networks

Mobile networks, such as GPRS, are not ready yet for large scale e-business applications as the bandwidth of today’s mobile networks is still too narrow. Still they offer many small incremental enhancements for corporate usage, such as packet switched data transfer, which enables new applications to be used. Wireless broadband networks are still to come and for example with today’s WLAN technologies it is too expensive to cover even a single large city and so they will not challenge 3G/UMTS networks, more likely they will complement each other in high traffic areas such as airports, railway stations and public buildings such as hotels, fair centres and conference halls.

8.2.3 Services

Services of mobile or wireless Internet will be a little different as they are and will be in fixed Internet due to the different kind of usage. Also the variety of different services will expand due to new technologies and what they may enable. Mobile services will be more personalized or they can be customized. How the adoption of the services will succeed will depend much on the pricing and on the other hand on the usefulness and easiness of usage. The lessons of WAP should have been learnt to prevent new set backs for expensive technologies. The hits of the new services will certainly be multimedia messaging and wireless instant messages; if not killed by too high pricing. As wireless instant messages posses a

threat to old and blooming SMS services, operators might be willing to hinder the march of new services that threaten their incomes.

Many of the current Web services will be made mobile. Giants like Microsoft and AOL Time Warner have already some mobile services in place for consumers to adopt. For the mobility users must pay some extra for those services. It is not so rare that the revenues from those services are then shared between the operator and the service provider.

As currently the most of the mobile services are already in the fixed web, the most important thing the mobility and wireless will add on this is the ubiquitous computing – web and services are available anywhere and anytime. The versatility of the mobile and wireless services will be increased due location and time based services.

8.2.4 Security

Security will be far more important as the possibilities for different scenarios arise due to the rise of the amount of the devices themselves. Also the wider scale of different terminal types and connection types will bring their own aspects to planning good security.

Also due to the nature of wireless, anyone can in theory listen to someone else's communications, it is recommendable not to rely purely on security provided by the networks themselves. As these things are known, security matters have to be solved out before businesses in wireless networks really start to happen. That is why it is easy to understand the success of VPN solutions as it is always advisable to use network independent security solutions, such as VPN, for extremely confidential data transfers.

Much of the security is about the users also with wireless technologies. Even when we could build a totally secure systems, one user could still easily cause a

leak in that system if he or she did not follow secure working methods; one could easily print classified documents from corporate intranet and then forget them into a public place like an airport lounge. Maybe the most important thing still is to educate the users the right attitude for security matters and remind them periodically: security starts from the user. In the wake of Internet time and the attacks against security many companies have risen to acknowledge the problems with security and have formed security policies. But still it seems that there has not been enough education as we just look back the last few years and think of all the viruses and worms spread through emails: people still open emails and attachments sent to them without hesitation. On the other hand in some companies the security measures might have been too restrictive that it even makes working more complex and inflexible. In many companies there has been absolute restriction of using PDAs in corporate networks as they might open security holes. It is easy to deny everything in the sake of security, but it also makes the users to try other ways round it and it can be even more hazardous.

8.2.5 Management

Managing the mobile enterprise will be a tough challenge for companies, and even tougher as the scale of different equipment will rise. And the multi network environment will definitely make the task even more complex. The management in this sense is not just managing the mobile equipment (hardware), it is also managing of technology, software, services of the company for its mobile personnel, security and how to combine all these efficiently and cost effectively.

Currently the markets lack good managerial services for implementation of PDAs into corporate usage. Currently there are solutions to bring mobile applications to mobile phones, but PDAs lack the same kind of services even though the technical possibilities already exist. Some pilots of that kind of services have already been made, but before it gets into wide spread use it will definitely take time. Also the currently available service packages are mostly suited for SMEs, not for large

corporation with thousands of employees. They still have to build their own systems and applications for mobile utilization.

8.3 Future visions

The future of wireless seems inevitable as the technologies mature and the prices will drop to a level at which every one can afford them. In the mobile phones this has already happened as the basic mobile phone costs some 150 €. Price drops in these entry models have slowed down, but the increase in features will continue in the future. Still, the newer the technology the more premium the customer has to pay for it but as the newer technologies gain more ground and mass markets the prices will drop to levels where they become common products.

In the future there will be a much wider range of service, many of them even unimaginable today. Digitalisation of services will change some things as we know them now. Already it is imaginable that video rental is going to bits as broadband networks are a commodity. Today we buy CDs but tomorrow it is possible we just buy access to that music from a service and then we hear the music whenever and wherever we want to.

As the technologies develop even the most fantasy like products or services may come true. What was yesterday a dream of a science fiction writer can be realised tomorrow as we have seen with one of the best known science fiction writers Jules Verne (1828-1905). Some of the inventions he imagined were created later in his lifetime, but some are still to be invented. He wrote over 80 books mostly before 1900 and a few of the things he described were: helicopters, modern weapons, movies with sound, television and rockets [AppleBookshop, 2001]. Today these inventions are just a part everyday life.

The following list entails what to expect in the development of technology in the next decades as the technologies are already in research.

2001 Wireless videophone
2002 Voice recognition
2002 Third generation mobile networks
2002 All phones Web-enabled
2003 Virtual retinal displays
2005 Wireless LAN standard on computers (integrated into computers)
2006 More wireless than fixed-phones
2007 Conversation with a computer
2008 Internet on Mars
2010 Internet appliances integrated to all kinds electric goods
2011 Fourth generation mobile networks
2015 Remote-controlled cars
2020 Holophone – 3D holographic moving images of people projected with mobile phones
2025 Mind reading
2030 Full, direct brain link

[Dornan, 2001, pp. 6-8]

Which of these will realize and which not, only the most rigorous critic, the time, will tell us. And definitely businesses are trying to adopt best of them to gain business efficiency, agility and flexibility.

8.4 Comments and recommendations

This study has focused mainly on the current wireless technologies and services and what they have for the companies. Important issues in this are the security of the technologies and how all this is managed.

In a study of this scale the technologies and services cannot be described in depth because also important security and management issues need to be covered. Each of these four main parts could constitute complete studies in themselves.

The case of mobile sales person is an interesting fore runner for the adoption of wireless technologies in a wider sense as it does not only include sales personnel in the usage of technologies, applications and services of that kind. The lessons learnt from that case can easily be applied to most of the mobile workforce.

At the moment the applications and services the mobile workforce would most probably need have just currently become available for different platforms (first office type of tools have already been on the market for a few years with SMS and WAP technologies). Newer technologies, such as XML and Java, are making the markets of these kind of services an interesting "battleground" to observe as the services are widely anticipated to be the drivers of the next generation networks.

The comparison between USA and Europe is also interesting to observe as till now both continents seemed to follow different technology evolution paths in mobile networks. In fall 2001 US operators AT&T wireless and Cingular Wireless announced that they have made a deal for GSM networks and showed trends towards a Europe-like evolution path to 3G. The pricing comparison of mobile telephoning and wireless services between the continents is also an interesting issue to look at as it has been widely accused that the US kind of charging of the receiver has hindered the development of US mobile markets. A third interesting comparison would be the security approaches of the continents. In Europe the security features have always played a role in user acceptance of services but in the US it has not been felt as needed as in Europe. The security of networks, devices, services, payments and all electronic communication has had lots of line space in the newspapers in the wake of 11th September 2001 terrorist attacks, which raised the nation to its toes.

9 SUMMARY

The goal of this study was to chart wireless technologies today and in next few years to come as well as the mobile services currently available in business-to-business and business-to-employee areas and their technology backgrounds. These technologies and services are viewed by the companies that will use them for their business purposes as well as taking into consideration what other matters it will bring to the companies that are adopting the new technologies and services, such as security issues and the corporate management issues of the wireless technologies, services and security.

In the theoretical part of the study the author investigated the drivers for the corporate adoption of new technologies such as wireless technologies but also the theoretical frameworks of wireless access technologies (networks and terminals), services (service technologies, service applications and service concepts) and security.

The empirical part consists of the management challenges the companies are facing when implementing wireless applications and a case example of a mobile sales person. The idea of the case is to show the reader how the technologies, services, security and management issues introduced earlier are handled in a real life application. The case is written using the technologies and services available currently. In the end the case is analysed and also recommendations for further development are given.

9.1 Conclusions

Wireless technologies bring many new possibilities for companies to achieve flexibility and competitiveness or even make possible things that were earlier impossible to do. The main obstacle in utilization of wireless technologies will be the imagination, or more importantly, the lack of it. But as the new technologies may sound a little heaven on Earth, they can become a nightmare if certain things

like security and the management of those technologies are not considered, planned and implemented well. For sure, these new technologies will reshape the ways of doing work, business or services, maybe not all, but many of them.

REFERENCES:

Andersson, Christoffer, 2001, GPRS and 3G Wireless Applications, John Wiley & Sons, Inc. ISBN 0-471-41405-0. 352p.

AppleBookshop, 2002. Jules Verne Biography. AppleBookshop Website [Referred: 25.1.2002] Available at:

Barbero, Manuel. 2001. Preparing to Ride the Wireless Wave. Journal of Business Strategy, September/October 2001, pp. 10-12.

Davies, Wynne, 2001. Wireless office on the move. International Telecommunications, October 2001, pp. 33-38.

Delta Wave, 2001. Delta Wave Products. Delta Wave Communications Inc. Website [Referred: 3.12.2001] Available at: http://www.deltawavecomm.com/ [Products]

DigiToday, 2002. GPRS ei pelitä ilman kiihdytinteknologiaa (in Finnish) [Referred: 18.02.2002] Available at: http://www.digitoday.fi/digi98fi.nsf/pub/te20020218141357_jvi_38319066

DoCoMo, 2001. i-Mode. NTT DoCoMo Website [Referred: 1.12.2001] Available at: http://www.nttdocomo.co.jp/english/ [products & services / i-mode]

Dornan, Andy, 2001. The Essential Guide to Wireless Communication Applications. Prentice Hall PTR, Upper Saddle River, NJ, USA. ISBN 0-13-031716-0. 315p.

Ericsson, 2002. LMDS – Wireless broadband access. Ericsson Corporate Website [Referred 26.2.2002] Available at: http://www.ericsson.com/transmission/wba/index.shtml#

Evans, Nicholas d., 2002. Business Agility: Strategies for Gaining Competitive Advantage through Mobile Business Solutions. Prentice Hall PTR, Upper Saddle River, NJ, USA. ISBN 0-13-066837-0. 247p.

eWeek, 2001. NTT DoCoMo Turns On 3G Network in Tokyo. eWeek (former Interactiveweek.com) news [Referred: 04.10.2001] Available at: http://www.eweek.com/article/0,3658,s=1884&a=15853,00.asp

Globalstar, 2001. Globalstar Products and Services. Globalstar Consortium Website [Referred: 4.12.2001] Available at: http://www.globalstar.com [Products & Services]

Hartman, Amir. Sifonis, John. Kador, John. 2000. Net Ready – Strategies for Success in the E-conomy. McGraw-Hill, New York, USA. ISBN 0-07-135242-2. 315p.

Hamel, Gary. 2000. Leading the revolution. Harvard Business School Press. Boston. ISBN 1-57851-189-5. 333p.

Holopainen, Sami. Lillrank, Paul. Paavola, Teemu. 1999. Tietotekniikan linkki liiketoimintaan. Otava. Keuruu. ISBN 951-1-16510-0. 183p. (in Finnish)

Haapala, Kari. ”VoiceXML”. Presentation held in the Tenth Summer School On Telecommunications, 8.8.2001, Lappeenranta.

Intel, 2002. Embedded Intel Architecture in Virtual Private Network Design White Paper. Intel Corporate Website [Referred: 17.2.2002] Available at: http://www.intel.com/platforms/applied/eiacomm/papers/vpn.htm

Iridium, 2002. Using Iridium – Services. Iridium Website [Referred: 24.1.2002] Avilable at: http://www.iridium.com/service/iri_service-detail.asp?serviceid=2

Kytölä, Olli & Edelmann, Jan, 2001. GPRS-data ei ole halpaa. MikroPC 17/2001, pp. 18.

Laaksonen, Petteri. Edelmann, Jan. Suikki, Petri. 2001 "Wireless E-Business Applications - Present Usage and New Application Opportunities in B2B Market", in Challenges of innovation and technology management for the new millennuim, Eds. Tuominen Markku, Torkkeli Marko, ISBN 951-764-558-9, 2001, pp. 177-184.

Leminen, Seppo. 1999. Gaps in Buyer-Seller Relationships – Case Studies in the Telecommunication Industry. Nr 77. Swedish School of Economics and Business Administration. Helsinki. ISBN 951-555-591-4. 354p.

Leung, Kenneth. Antypas, John. 2001. Improving returns on M-Commerce investments. Journal of Business Strategies, September/October 2001, pp. 12-13.

Liberty Alliance, 2001. Liberty Alliance Project. Liberty Alliance Website [Referred: 4.12.2001] Available at: http://www.projectliberty.org/

Microsoft, 2001. Microsoft .NET. Microsoft Corporate Website. [Referred: 25.11.2001] Available at: http://www.microsoft.com/net/

MPRG, 2001, “2G, 2.5G and 3G systems”, Research paper, The Mobile and Portable Radio Research Group at Virginia Tech [Referred 14.10.2001] Available at: http://www.mprg.org/research/4gwg/2Gand25GSystems/2_5G.pdf

Müller-Veerse, Falk. 1999. Mobile Commerce Report. Durlacher Research Ltd. 77p.

Müller-Veerse et al.. 2001. UMTS report – An Investment Perspective. Durlacher Research Ltd. 141p.

Nokia, 2001a. WAP on Web. Nokia Corporate Website [Referred: 27.10.2001] Available at: http://www.nokia.com/wap/wap.html

Nokia, 2001b. MMS. Nokia Corporate Website [Referred: 15.11.2001] Available at: http://www.nokia.com/mms/index.html

Nokia, 2001c. Industry leaders announce commitment to open mobile architecture enabling a non-fragmented global mobile services market, [Press Release - document] Nokia Corporate Communications [Referred: 18.11. 2001] Available at: http://press.nokia.com/PR/200111/840158_5.html

Paavilainen, Jouni. 2001. Mobile Commerce Strategies. IT Press. ISBN 951-826-253-5. 252p.

Parker, T. and McQueen, D. 2001. Content & Applications for the Wireless Internet, Worldwide Market Analysis & Strategic Outlook 2001-2006, ARC Group, Surrey. ISBN 1-902-740-122. 260p.

Remenyi, Dan & Money, Arthur & Twite, Alan. 1991. A guide to measuring and managing IT benefits. Oxford: TechTrans Limited. ISBN 1-85554-138-6. 299 p.

Rousku, Kimmo, 2001. Microsoft .Net yrittää tarjota kaikille kaikkea. MicroPC 14/2001 pp. 44-45

Schneier, Bruce, 2000, Secrets and Lies, Digital Security in a Networked World, John Wiley & Sons, Inc. ISBN 0-471-25311-1. 412p.

Sharma, Chetan, 2001, Wireless Internet Enterprise Applications, John Wiley & Sons, Inc. ISBN 0-471-39382-7. 236p.

Snellman, Kalle, 2001, Nordic Mobile Services and mCommerce 2000 – 2005. IDC. IDC# N540160H. 76p.

Teledesic, 2002. About Teledesic. Teledesic Corporate Website [Referred: 9.3.2002] Available at: http://www.teledesic.com/about/about.htm

Tiainen, Olli-Pekka, 2001, GPRS-ruletti kiihtyy, (in Finnish), Taloussanomat 3.10.2001, pp. 21

Total Romtec. 2000. Corporate Mobile Data – the business market for mobile Internet applications. October 2000. 68p.

UMTS Forum. 2001. Report No. 13, The UMTS third generation market – Phase II: Structuring the service revenue opportunities. 100p.
Ward, Ellen. 1998. World-class telecommunications service development. Artech House. ISBN 0-89006-922-0. 260p.

Vaultus, 2001. Vaultus Mobile Platform – Vaultus Technical White Paper. Vaultus Corporate Website. [Referred: 27.11.2001] Available at: http://www.vaultus.com/solutions/document.html

WATMAG, 2001. EDGE Protocol Analysis. Wireless Access Technologies [Referred: 20.11.2001] Avalable at: http://www.watmag.com/technologies/GPRS_EDGE/GPRS-005.html

Whatis?com, 2002a. IPsec. Whatis?com Definitions [Referred: 14.2.2002] Available at: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214037,00.html

Whatis?com, 2002a. Cryptography. Whatis?com Definitions [Referred: 16.2.2002] Available at: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214431,00.html

Webopedia, 2001, "3G Definition", Webopedia: Online Dictionary for Computer and Internet Terms [Referred 11.10.2001] Available at http://webopedia.internet.com/TERM/3/3G.html

VERBAL REFERENCES:

Annala, Timo, CTO, Sonera Corporation, Interview in Helsinki 23.08.2001

Huhtala, Petri, Product group manager, Sonera Corporation, Interview in Helsinki 03.10.2001

Häyrynen, Jouko, Vice president, Nokia Mobile Phones, Interview in Espoo, 06.09.2001

Impivaara, Matias, Manager – product marketing, F-Secure, Interview in Helsinki 22.08.2001

Koffert, Kalle, Development manager, Sonera Corporation, Interview in Helsinki 16.01.2002

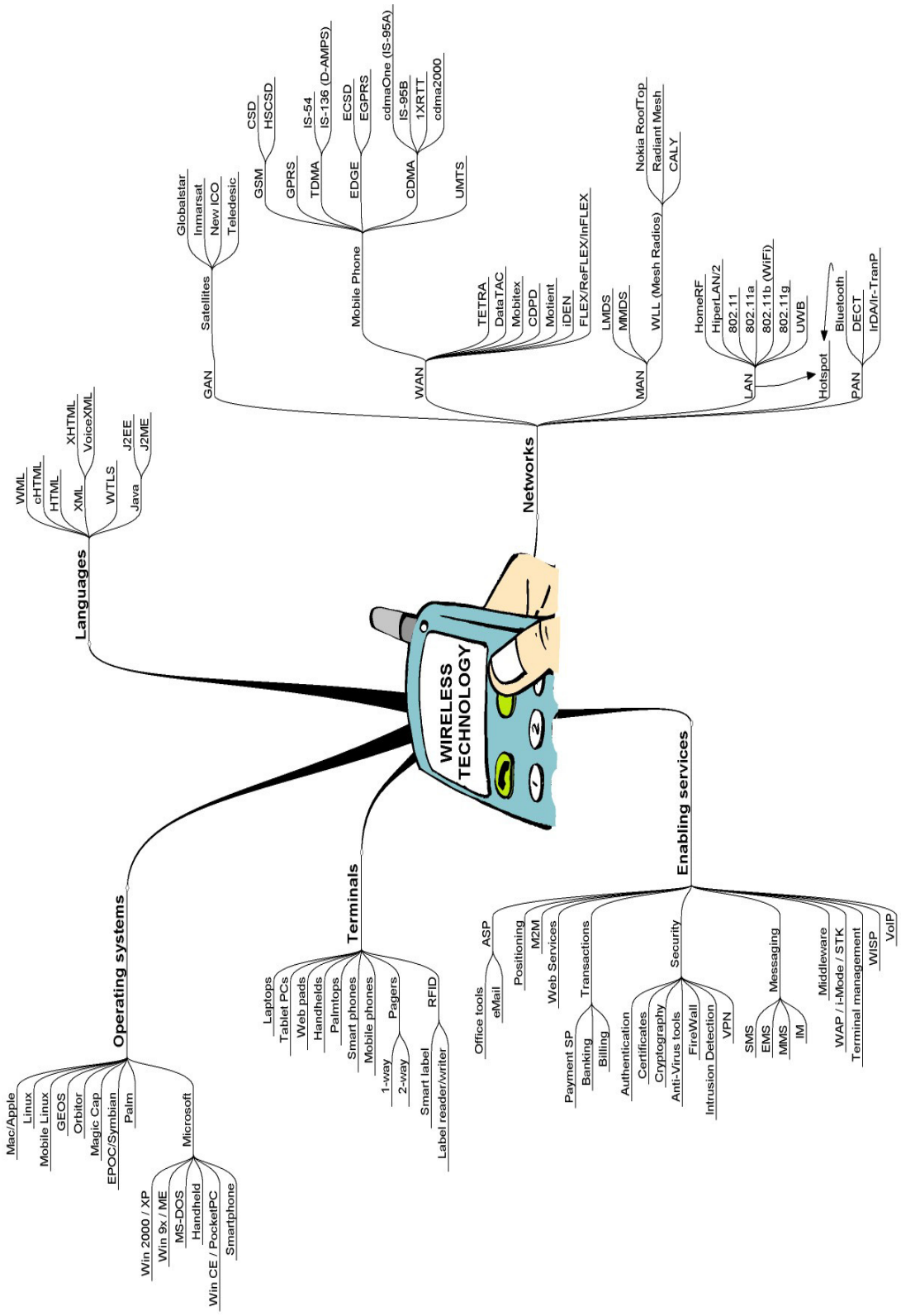
Lönnqvist, Kurt, Manager – e-Business solutions, IBM, Interview in Helsinki 10.09.2001

Mikkonen, Jussi, Head of global deliveries & product management, Sonera Zed ltd, Interview in Helsinki, 14.12.2001

Parkkali, Petri, Department manager, Novo group, Presentation at "Automaatio Messut 2001" in Helsinki, 06.09.2001

Sandstedt, Ari, Development director, Sonera Corporation, Interview in Helsinki 23.08.2001

APPENDIX I: Wireless Technology Landscape



APPENDIX II: Network technologies

Technology	**Transfer rates**	**Max cell radius**	**Frequency band**
Bluetooth	Up to 1 Mbps	10 m, 100 with amp	2.4 GHz
IrDA	115 kbps – 4 Mbps	1 m + line of sight	Infrared light
IEEE 802.11	1 – 2 Mbps	10 – 500 m	2.4 GHz
IEEE 802.11a	Up to 54 Mbps	5 km	5 – 6 GHz
IEEE 802.11b	2.4 – 11 Mbps	10 – 500 m	2.4 GHz
IEEE 802.11g	At least 20 Mbps	10 – 500 m	2.4 GHz
HomeRF	Up to 1.6 Mbps	Up to 50 m	2.4 GHz
HomeRF 2.0	Up to 10 Mbps	Up to 50 m	2.4 GHz
HiperLAN	Up to 20 Mbps	10 – 200 m	5 GHz
HiperLAN/2	Up to 54 Mbps	10 – 200 m	5 GHz
GSM	9.6 kbps	30 km	900 / 1800 MHz
HSCSD	14.4 – 57.6 kbps	20 km	900 / 1800 MHz
GPRS	Up to 171.2 kbps	10 km	900 / 1800 MHz
EDGE	Up to 384 kbps	10 km	900 / 1800 MHz
UMTS	Up to 2 Mbps	5 km	1.9 – 2.2 GHz
LMDS	Up to 155 Mbps	1 – 8 km	28 GHz
Satellite system	***Transfer rates***	***Satellites***	
Iridium	Up to 10 kbps	66	
Globalstar	Up to 9.6 kbps	48	
Teledesic	Up to 64 Mbps	288 + 36	

APPENDIX III: Acronyms

1G: First generation mobile communication system

2G: Second generation mobile communication systems

3G: Third generation mobile communication system

3GPP: Third Generation Partnership Project

A-GPS: Assisted Global Positioning System

AHP: Analytic Hierarchy Process

AMPS: Advanced Mobile Phone Service

AOL: America OnLine

API: application program interface

ASP: Application Service Provider

B2B: Business-to-Business

B2C: Business-to-Consumer

B2E: Business-to-Employee

CDMA: Code Division Multiple Access

CDPD: Cellular Digital Packet Data

cHTML: Compact HTML

COO: Cell of Origin

CPU: Central Processing Unit

CRM: Customer Relationship Management

DECT: Digital Enhanced Cordless Telecommunications

EAI: Enterprise Application Integration

EDGE: Enhanced Data Rates for Global Evolution

EMS: Enhanced Message Service

ERP: Enterprise Resource Planning

E-TDMA: Extended Time Division Multiple Access

ETSI: European Telecommunication Standards Institute

FCC: Federal Communications Commission

FTP: File Transfer Protocol

FWBA: Fixed Wireless Broadband Access

GAN: Global Area Network

GPRS: General Packet Radio Service

GPS: Global Positioning System

GSM: Global System for Mobile Communications

HiperLAN: High Performance Radio Local Area Network

HMS: Horizontal Management Services

HMSP: Horizontal Management Services Provider

HSCSD: High Speed Circuit Switched Data

HTML: Hypertext Markup Language

ICT: Information and Communications Technology

ICQ: "I Seek You"

IEEE: Institute of Electric and Electronic Engineers

APPENDIX III: Acronyms

IM: Instant Messaging

IP: Internet Protocol

IPsec: Internet Protocol security

IPv6: Internet Protocol version 6

IrDA: Infrared Data Association

IRC: Internet Relay Chat

ISP: Internet Service Provider

IT: Information Technology

LAN: Local Area Network

LEO: Low Earth Orbit

LMDS: Local Multipoint Distribution Service

M2M: Machine-to-Machine

MAC: Media Access Control

MASP: Mobile Application Service Provider

M-CRM: Mobile Customer Relations Management

MDSS: Mobile Data Synchronization Service

MLS: Mobile Location Service

MMS: Multimedia Message Service

M-SCM: Mobile Supply Chain Management

MSN: Microsoft Network

OS: Operating System

OSI: Open Systems Interconnection

OWLAN: Operator Wireless LAN

PAN: Personal area network

PCMCIA: Personal Computer Memory Card International Association

PDA: Personal Digital Assistant

PDC: Personal Digital Communications

PDN: Public data network / Packet-data network

PIN: Personal Identification Number

PIM: Personal Information Management

PKI: Public Key Infrastructure

PSTN: Public Switched Telephone Network

RF: Radio Frequency

RSA: Rivest – Shamir - Adleman

SIM: Subscriber Identity Module

SCM: Supply Chain Management

SMS: Short Message Service

SP: Service Provider

SSH: Secure Shell

SSL: Secure Socket Layer

TBRC: Telecom Business Research Center

TCP/IP: Transmission Control Protocol / Internet Protocol

TD/CDMA: Time Division/Code Division Multiple Access

TDMA: Time Division Multiple Access

APPENDIX III: Acronyms

UDP: User Datagram Protocol

UMTS: Universal Mobile Telephone System

USB: Universal Serial Bus

VAS: Value Added Services

VoIP: Voice over Internet Protocol

VPN: Virtual Private Network

W3C: World Wide Web Consortium

WAN: Wide Area Network

WAP: Wireless Application Protocol

WCDMA: Wideband Code Division Multiple Access

WEP: Wired Equivalent Privacy

WiFi: Wireless Fidelity

WIM: Wireless Instant Messaging

WLAN: Wireless Local Access Network

WML: Wireless Markup Language

WSP: Wireless Service Provider

W-TDMA: Wideband Time Division Multiple Access

WWW: World Wide Web

XHTML: eXtensible Hyper Text Markup Language

XML: Extensible Markup Language